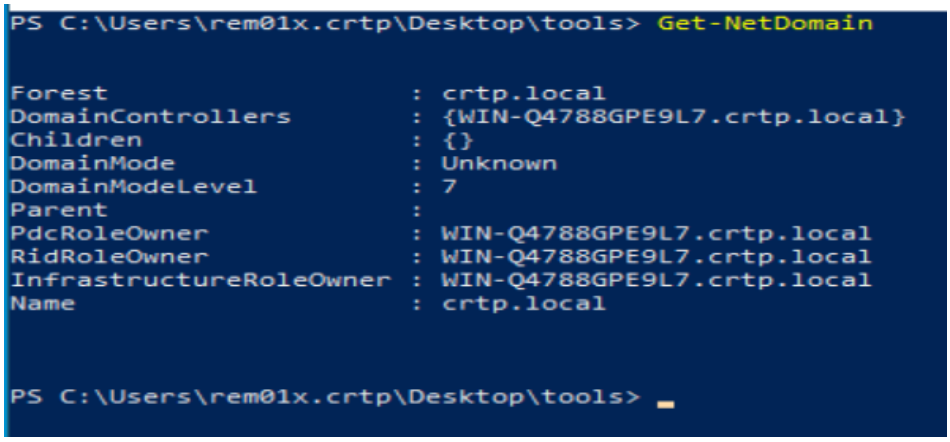
Powerview

Loading Powerview

```
. .\powerview.ps1
```

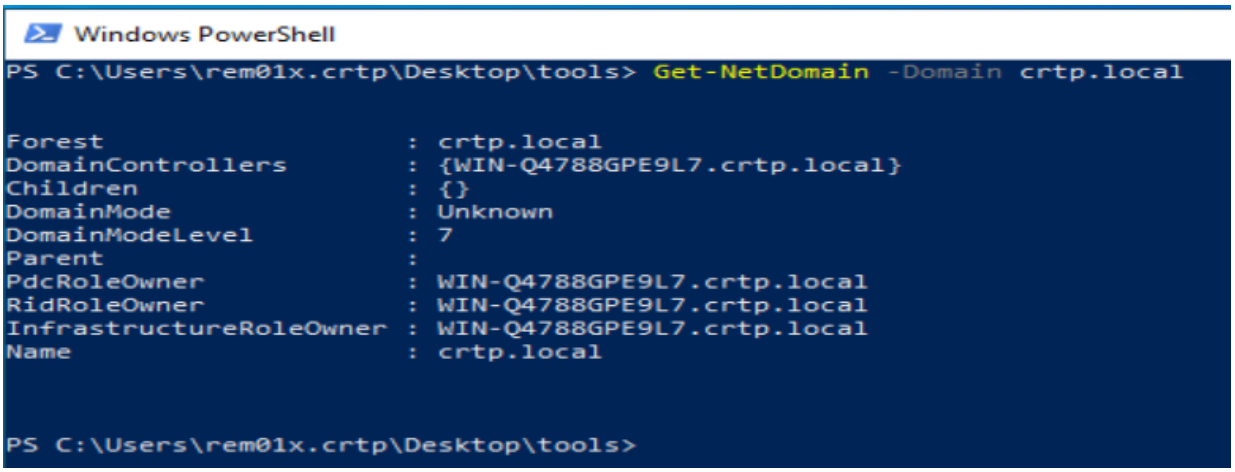
now getting the current domain information

```
Get-NetDomain
```



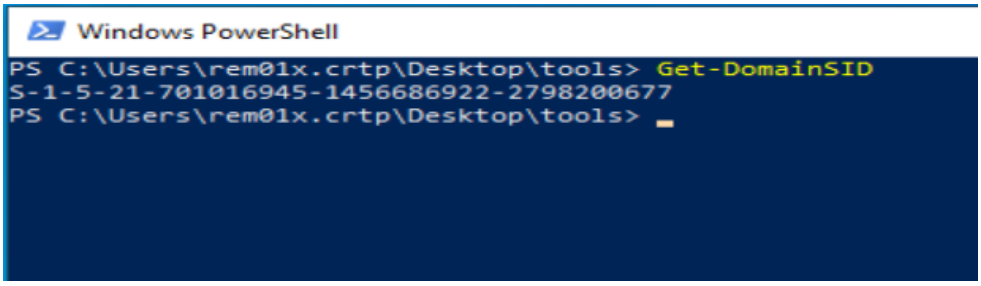
Getting Info from another domain if we have trusts

```
Get-NetDomain -Domain crtp.local
```



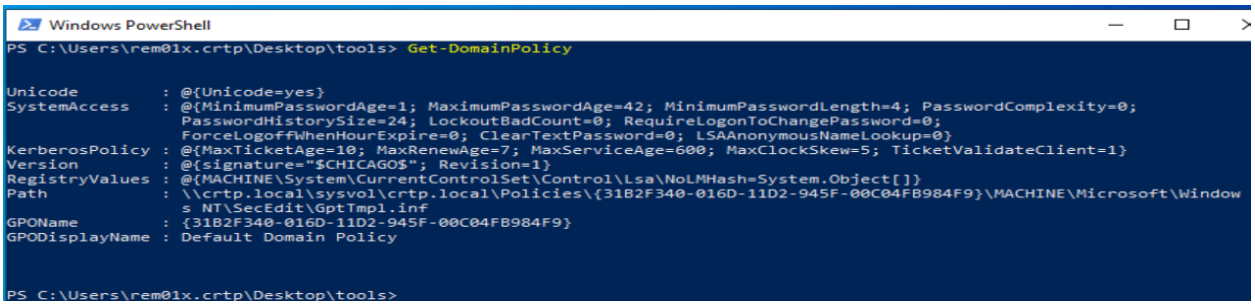
getting the domainSID

```
Get-DomainSID
```



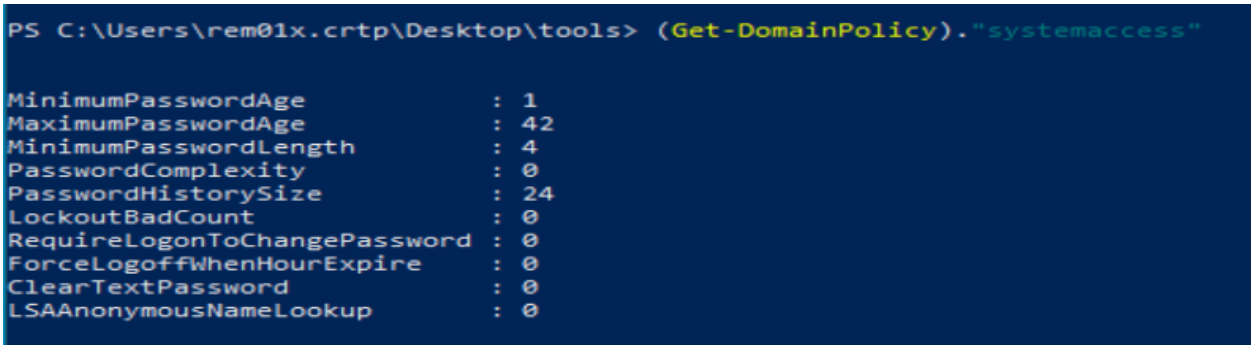
getting domain policy

```
Get-DomainPolicy
```



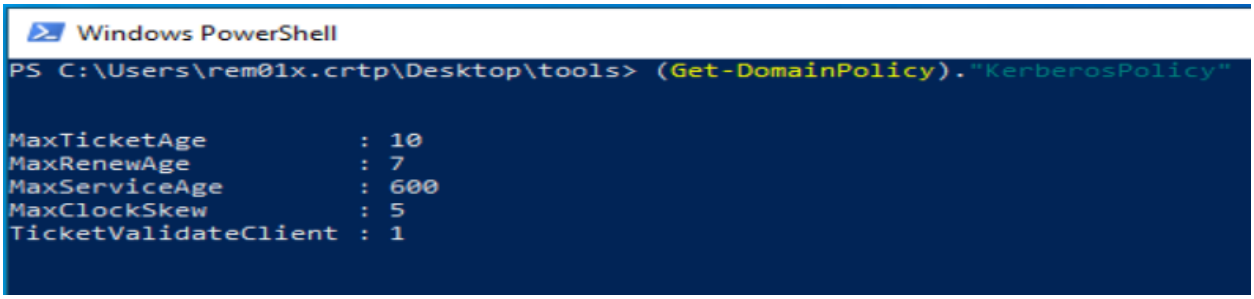
getting system access policy

```
(Get-DomainPolicy)."systemaccess"
```



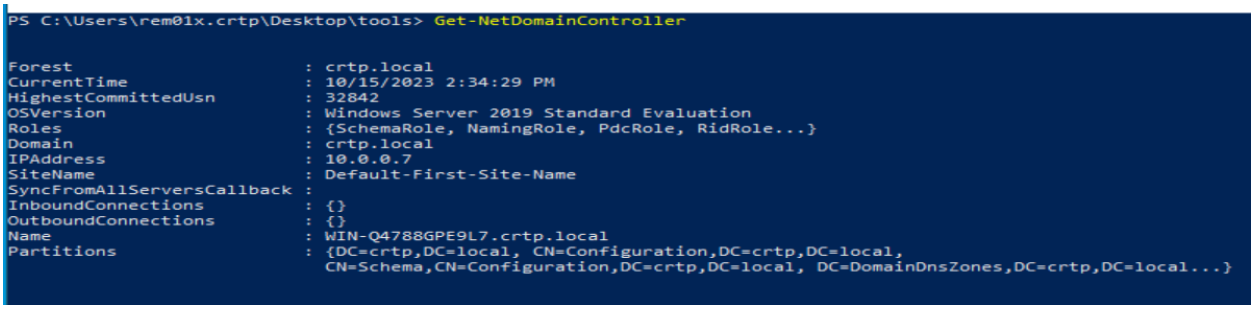
getting kerberos policy

```
(Get-DomainPolicy)."KerberosPolicy"
```



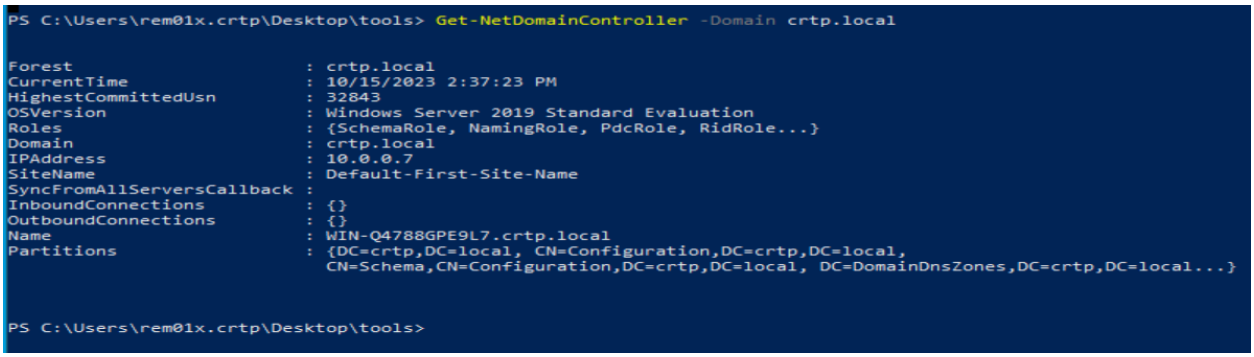
getting information about the domain controller

```
Get-NetDomainController
```



getting information about the domain controller of another domain if we have trusts

```
Get-NetDomainController -Domain crtp.local
```



getting domain users

```
Get-NetUser
```

```
logoncount              : 11
badpasswordtime         : 1/1/1601 2:00:00 AM
distinguishedname       : CN=rem01x,CN=Users,DC=crtp,DC=local
objectclass             : {top, person, organizationalPerson, user}
lastlogontimestamp      : 10/15/2023 2:46:05 PM
userprincipalname       : rem01x@crtp.local
name                    : rem01x
objectsid               : S-1-5-21-701016945-1456686922-2798200677-1455
samaccountname          : rem01x
codepage                : 0
samaccounttype          : USER_OBJECT
accountexpires          : NEVER
countrycode             : 0
whenchanged             : 10/15/2023 12:46:05 PM
instancetype            : 4
usncreated              : 24620
objectguid              : 85e5a49b-19bd-4203-aacf-1d7bddd4ac6c
sn                      : rem01x
lastlogoff              : 1/1/1601 2:00:00 AM
objectcategory          : CN=Person,CN=Schema,CN=Configuration,DC=crtp,DC=local
dscorepropagationdata   : 1/1/1601 12:00:00 AM
givenname               : rem01x
lastlogon               : 10/15/2023 4:12:24 PM
badpwdcount             : 0
cn                      : rem01x
useraccountcontrol      : NORMAL_ACCOUNT
whencreated             : 10/15/2023 12:45:52 PM
primarygroupid          : 513
pwdlastset              : 10/15/2023 2:45:52 PM
usnchanged              : 24625
```

getting users cn name

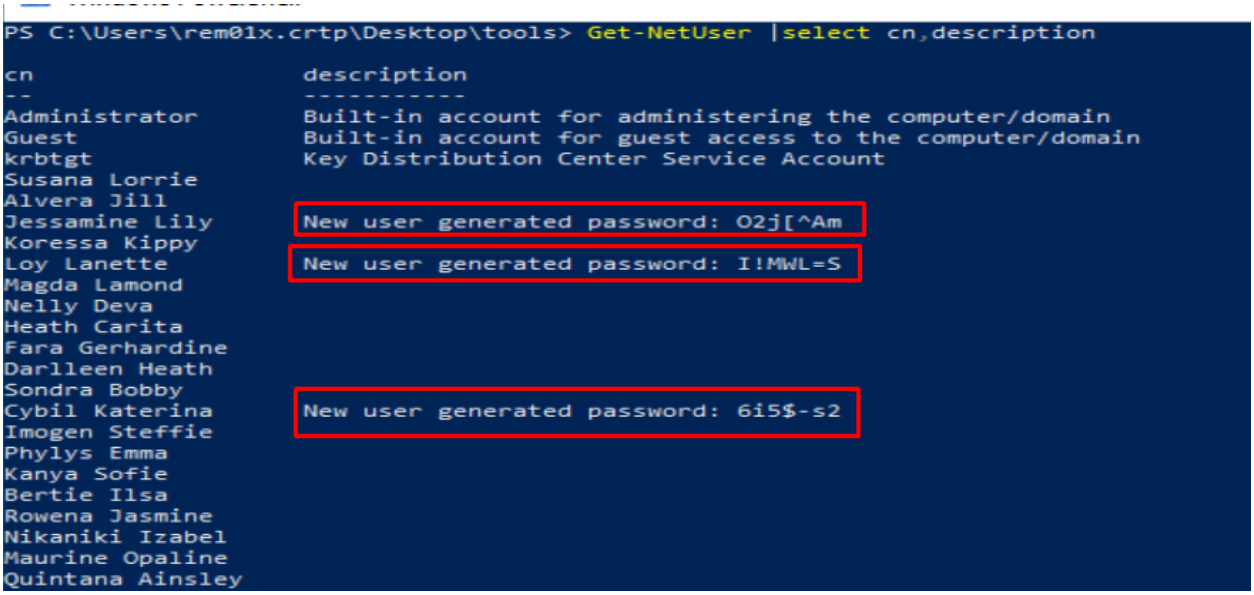
```
Get-NetUser | select cn
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetUser |select cn

cn
--
Administrator
Guest
krbtgt
Susana Lorrie
Alvera Jill
Jessamine Lily
Koressa Kippy
Loy Lanette
Magda Lamond
Nelly Deva
Heath Carita
Fara Gerhardine
Darlleen Heath
Sondra Bobby
Cybil Katerina
Imogen Steffie
Phylys Emma
Kanya Sofie
Bertie Ilsa
Rowena Jasmine
Nikaniki Izabel
Maurine Opaline
Quintana Ainsley
Perry Sheilah
Rozanne Ortensia
```

getting cn name and description

```
Get-NetUser | select cn,description
```



as we see we found some passwords in the description area

now let's take a look at all those users

```
Billie Caitlin      DNS Admin
Nona Donetta        Company default password(Reset ASAP)
Cymbre Goldina      New user generated password: sDjr$!E
Dayle Kelcey        Company default password(Reset ASAP)
Aloysia Debbie      New user generated password: m:{jWvi
Illa Latashia       Company default password(Reset ASAP)
Lanette Kitty       Company default password(Reset ASAP)
Haleigh Shirlene    DNS Admin
Elenore Brandie     Company default password(Reset ASAP)
Delilah Alyss       Company default password(Reset ASAP)
Kimberlee Lorna     Company default password(Reset ASAP)
Reyna Ninon         New user generated password: B&wh/^#
Cybil Katerina      New user generated password: 6i5$-s2
Loy Lanette         New user generated password: I!MWL=S
Jessamine Lily      New user generated password: O2j[^Am
```

taking a look at password last set

```
Get-NetUser | select cn,description,badpwdcount,pwdlastset
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetUser | select cn,description,badpwdcount,pwdlastset

cn                  description                                                  badpwdcount pwdlastset
--                  -----------                                                  ----------- ----------
Administrator       Built-in account for administering the computer/domain               984 10/14/2023 10:38:51 PM
Guest               Built-in account for guest access to the computer/domain               0 1/1/1601 2:00:00 AM
krbtgt              Key Distribution Center Service Account                              984 10/14/2023 10:47:00 PM
Susana Lorrie                                                                              0 10/14/2023 10:54:07 PM
Alvera Jill                                                                                0 1/1/1601 2:00:00 AM
Jessamine Lily      New user generated password: O2j[^Am                                   0 1/1/1601 2:00:00 AM
Koressa Kippy                                                                              0 10/14/2023 10:54:07 PM
Loy Lanette         New user generated password: I!MWL=S                                   0 1/1/1601 2:00:00 AM
Magda Lamond                                                                               0 10/14/2023 10:54:07 PM
Nelly Deva                                                                                 0 10/14/2023 10:54:07 PM
Heath Carita                                                                               0 10/14/2023 10:54:07 PM
Fara Gerhardine                                                                            0 10/14/2023 10:54:07 PM
Darlleen Heath                                                                             0 1/1/1601 2:00:00 AM
Sondra Bobby                                                                               0 10/14/2023 10:54:07 PM
Cybil Katerina      New user generated password: 6i5$-s2                                   0 1/1/1601 2:00:00 AM
Imogen Steffie                                                                             0 10/14/2023 10:54:08 PM
Phylys Emma                                                                                0 1/1/1601 2:00:00 AM
Kanya Sofie                                                                                0 10/14/2023 10:54:08 PM
Bertie Ilsa                                                                                0 10/14/2023 10:54:08 PM
Rowena Jasmine                                                                             0 10/14/2023 10:54:08 PM
Nikaniki Izabel                                                                            0 10/14/2023 10:54:08 PM
Maurine Opaline                                                                            0 10/14/2023 10:54:08 PM
Quintana Ainsley                                                                           0 10/14/2023 10:54:08 PM
```

we take a look at those because there maybe any decoys that can be used as a trap for hackers

```
Get-NetUser | select cn,logoncount
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetUser | select cn,logoncount

cn                  logoncount
--                  ----------
Administrator               15
Guest                        0
krbtgt                       0
Susana Lorrie                0
Alvera Jill                  0
Jessamine Lily               0
Koressa Kippy                0
Loy Lanette                  0
Magda Lamond                 0
Nelly Deva                   0
Heath Carita                 0
Fara Gerhardine              0
Darlleen Heath               0
Sondra Bobby                 0
Cybil Katerina               0
```

getting information about computers in the domain

```
Get-NetComputer
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetComputer


pwdlastset                    : 10/14/2023 10:47:17 PM
logoncount                    : 24
serverreferencebl             : CN=WIN-Q4788GPE9L7,CN=Servers,CN=Default-First-Site-Name,C
badpasswordtime               : 1/1/1601 2:00:00 AM
distinguishedname             : CN=WIN-Q4788GPE9L7,OU=Domain Controllers,DC=crtp,DC=local
objectclass                   : {top, person, organizationalPerson, user...}
lastlogontimestamp            : 10/14/2023 10:47:38 PM
name                          : WIN-Q4788GPE9L7
objectsid                     : S-1-5-21-701016945-1456686922-2798200677-1000
samaccountname                : WIN-Q4788GPE9L7$
localpolicyflags              : 0
codepage                      : 0
samaccounttype                : MACHINE_ACCOUNT
whenchanged                   : 10/14/2023 9:00:35 PM
accountexpires                : NEVER
countrycode                   : 0
operatingsystem               : Windows Server 2019 Standard Evaluation
instancetype                  : 4
msdfsr-computerreferencebl    : CN=WIN-Q4788GPE9L7,CN=Topology,CN=Domain System Volume,CN=
objectguid                    : fd11ef97-abba-4136-9f90-9f6adb95ac78
operatingsystemversion        : 10.0 (17763)
lastlogoff                    : 1/1/1601 2:00:00 AM
objectcategory                : CN=Computer,CN=Schema,CN=Configuration,DC=crtp,DC=local
dscorepropagationdata         : {10/14/2023 8:47:00 PM, 1/1/1601 12:00:01 AM}
serviceprincipalname          : {Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/WIN-Q4788GPE9L7
                                ldap/WIN-Q4788GPE9L7.crtp.local/ForestDnsZones.crtp.local,
                                ldap/WIN-Q4788GPE9L7.crtp.local/DomainDnsZones.crtp.local,
```

now we may filter the cn and the operating system of the computer

```
Get-NetComputer | select cn,operatingsystem
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetComputer | select cn,operatingsystem

cn               operatingsystem
--               ---------------
WIN-Q4788GPE9L7 Windows Server 2019 Standard Evaluation
DESKTOP-V0AN63P Windows 10 Pro N


PS C:\Users\rem01x.crtp\Desktop\tools>
```

getting operating system (os) information

```
Get-NetComputer -OperatingSystem "*server*" |select cn,operatingsystem
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetComputer -OperatingSystem "*server*" |select cn,operatingsystem

cn             operatingsystem
--             ---------------
WIN-Q4788GPE9L7 Windows Server 2019 Standard Evaluation
```

note: finding a computer object in the active directory does not mean that this object must be connected with a real computer or server

checking live machines

```
Get-NetComputer -Ping
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetComputer -Ping


pwdlastset                    : 10/14/2023 10:47:17 PM
logoncount                    : 24
serverreferencebl             : CN=WIN-Q4788GPE9L7,CN=Servers,CN=Default-First-Site-Name,CN=S
                                =local
badpasswordtime               : 1/1/1601 2:00:00 AM
distinguishedname             : CN=WIN-Q4788GPE9L7,OU=Domain Controllers,DC=crtp,DC=local
objectclass                   : {top, person, organizationalPerson, user...}
lastlogontimestamp            : 10/14/2023 10:47:38 PM
name                          : WIN-Q4788GPE9L7
objectsid                     : S-1-5-21-701016945-1456686922-2798200677-1000
samaccountname                : WIN-Q4788GPE9L7$
localpolicyflags              : 0
codepage                      : 0
samaccounttype                : MACHINE_ACCOUNT
whenchanged                   : 10/14/2023 9:00:35 PM
accountexpires                : NEVER
countrycode                   : 0
operatingsystem               : Windows Server 2019 Standard Evaluation
instancetype                  : 4
msdfsr-computerreferencebl    : CN=WIN-Q4788GPE9L7,CN=Topology,CN=Domain System
                                Volume,CN=DFSR-GlobalSettings,CN=System,DC=crtp,DC=local
objectguid                    : fd11ef97-abba-4136-9f90-9f6adb95ac78
operatingsystemversion        : 10.0 (17763)
lastlogoff                    : 1/1/1601 2:00:00 AM
objectcategory                : CN=Computer,CN=Schema,CN=Configuration,DC=crtp,DC=local
```

getting information about groups

```
Get-NetGroup
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGroup


grouptype                : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY
admincount               : 1
iscriticalsystemobject   : True
samaccounttype           : ALIAS_OBJECT
samaccountname           : Administrators
whenchanged              : 10/15/2023 12:53:50 PM
objectsid                : S-1-5-32-544
objectclass              : {top, group}
cn                       : Administrators
usnchanged               : 24701
systemflags              : -1946157056
name                     : Administrators
```

more visable info

```
Get-NetGroup | select cn,member
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGroup | select cn,member

cn                                             member
--                                             ------
Administrators                                 {CN=Domain Admins,CN=Users,DC=crtp,
Users                                          {CN=Domain Users,CN=Users,DC=crtp,D
Guests                                         {CN=Domain Guests,CN=Users,DC=crtp,
Print Operators
Backup Operators
Replicator
Remote Desktop Users
Network Configuration Operators
Performance Monitor Users
Performance Log Users
Distributed COM Users
IIS_IUSRS                                      CN=S-1-5-17,CN=ForeignSecurityPrinc
Cryptographic Operators
Event Log Readers
Certificate Service DCOM Access
RDS Remote Access Servers
RDS Endpoint Servers
RDS Management Servers
Hyper-V Administrators
Access Control Assistance Operators
Remote Management Users
Storage Replica Administrators
Domain Computers
Domain Controllers
Schema Admins                                  CN=Administrator,CN=Users,DC=crtp,D
```

getting group info for another domain if we have trusts

```
Get-NetGroup -Domain crtp.local
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGroup -Domain crtp.local


grouptype              : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY
admincount             : 1
iscriticalsystemobject : True
samaccounttype         : ALIAS_OBJECT
samaccountname         : Administrators
whenchanged            : 10/15/2023 12:53:50 PM
objectsid              : S-1-5-32-544
objectclass            : {top, group}
cn                     : Administrators
usnchanged             : 24701
systemflags            : -1946157056
name                   : Administrators
dscorepropagationdata  : {10/15/2023 12:53:50 PM, 10/14/2023 8:47:00 PM, 1/1/160
description            : Administrators have complete and unrestricted access to
distinguishedname      : CN=Administrators,CN=Builtin,DC=crtp,DC=local
member                 : {CN=Domain Admins,CN=Users,DC=crtp,DC=local, CN=Enterpr
                         CN=Administrator,CN=Users,DC=crtp,DC=local}
usncreated             : 8199
whencreated            : 10/14/2023 8:46:06 PM
instancetype           : 4
```

getting information about specific groups

```
Get-NetGroup 'IT Admins'
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGroup 'IT Admins'


usncreated             : 13199
admincount             : 1
grouptype              : GLOBAL_SCOPE, SECURITY
samaccounttype         : GROUP_OBJECT
samaccountname         : IT Admins
whenchanged            : 10/15/2023 12:53:50 PM
objectsid              : S-1-5-21-701016945-1456686922-2798200677-1204
objectclass            : {top, group}
cn                     : IT Admins
usnchanged             : 24676
dscorepropagationdata  : {10/15/2023 12:53:50 PM, 10/14/2023 9:05:48 PM, 10/14/2023 9:05:41 PM, 10/14/2023 9:05:41 PM...}
memberof               : CN=Domain Admins,CN=Users,DC=crtp,DC=local
distinguishedname      : CN=IT Admins,CN=Users,DC=crtp,DC=local
name                   : IT Admins
member                 : {CN=Luise Lenna,CN=Users,DC=crtp,DC=local, CN=Lilas Kip,CN=Users,DC=crtp,DC=local, CN=Marlee
                         Charlot,CN=Users,DC=crtp,DC=local, CN=Darleen Noreen,CN=Users,DC=crtp,DC=local...}
whencreated            : 10/14/2023 8:54:12 PM
instancetype           : 4
objectguid             : 14315080-e179-465a-b45a-0835ffbb210a
objectcategory         : CN=Group,CN=Schema,CN=Configuration,DC=crtp,DC=local
```

enumerating specific group in other domain if we have trusts

```
Get-NetGroup -Domain crtp.local 'IT Admins'
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGroup -Domain crtp.local 'IT Admins'


usncreated             : 13199
admincount             : 1
grouptype              : GLOBAL_SCOPE, SECURITY
samaccounttype         : GROUP_OBJECT
samaccountname         : IT Admins
whenchanged            : 10/15/2023 12:53:50 PM
objectsid              : S-1-5-21-701016945-1456686922-2798200677-1204
objectclass            : {top, group}
cn                     : IT Admins
usnchanged             : 24676
dscorepropagationdata  : {10/15/2023 12:53:50 PM, 10/14/2023 9:05:48 PM, 10/14/2023 9:05:41 PM, 10/14/2023 9:05:41
                         PM...}
memberof               : CN=Domain Admins,CN=Users,DC=crtp,DC=local
distinguishedname      : CN=IT Admins,CN=Users,DC=crtp,DC=local
name                   : IT Admins
member                 : {CN=Luise Lenna,CN=Users,DC=crtp,DC=local, CN=Lilas Kip,CN=Users,DC=crtp,DC=local, CN=Marlee
                         Charlot,CN=Users,DC=crtp,DC=local, CN=Darleen Noreen,CN=Users,DC=crtp,DC=local...}
whencreated            : 10/14/2023 8:54:12 PM
instancetype           : 4
objectguid             : 14315080-e179-465a-b45a-0835ffbb210a
objectcategory         : CN=Group,CN=Schema,CN=Configuration,DC=crtp,DC=local
```

using a wildcard in group name

```
Get-NetGroup *admin* | select cn
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGroup *admin* | select cn

cn
--
Administrators
Hyper-V Administrators
Storage Replica Administrators
Schema Admins
Enterprise Admins
Domain Admins
Key Admins
Enterprise Key Admins
DnsAdmins
Office Admin
IT Admins
```

getting information about group members

```
Get-NetGroupMember 'IT Admins' -Recurse | select membername
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGroupMember 'It Admins' -Recurse | select membername

MemberName
----------
luise.lenna
lilas.kip
marlee.charlot
darleen.noreen
prissie.alice
gratia.jillayne
aida.gratiana
riki.lynnell
shelba.casandra
sabra.franky
kalie.giana
paloma.raeann
dorena.athena
christyna.dorothy
kinnie.fiann
althea.devan
rosy.libbey
rowena.jasmine
```

getting the groups that the user is member of

```
Get-NetGroup -UserName rem01x | select name
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGroup -UserName rem01x | select name

name
----
Domain Users


PS C:\Users\rem01x.crtp\Desktop\tools> _
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGroup -UserName shelba.casandra | select name

name
----
Denied RODC Password Replication Group
Domain Admins
Domain Users
IT Admins
```

enumerating the local groups of the machine require administrative access on non dc machines

```
Get-NetLocalGroup -ComputerName WIN-Q4788GPE9L7
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetLocalGroup -ComputerName WIN-Q4788GPE9L7

ComputerName     GroupName                                Comment
------------     ---------                                -------
WIN-Q4788GPE9L7 Server Operators                          Members can administer domain s
WIN-Q4788GPE9L7 Account Operators                         Members can administer domain u
WIN-Q4788GPE9L7 Pre-Windows 2000 Compatible Access        A backward compatibility group
WIN-Q4788GPE9L7 Incoming Forest Trust Builders            Members of this group can creat
WIN-Q4788GPE9L7 Windows Authorization Access Group        Members of this group have acce
WIN-Q4788GPE9L7 Terminal Server License Servers           Members of this group can updat
WIN-Q4788GPE9L7 Administrators                            Administrators have complete an
WIN-Q4788GPE9L7 Users                                     Users are prevented from making
WIN-Q4788GPE9L7 Guests                                    Guests have the same access as
WIN-Q4788GPE9L7 Print Operators                           Members can administer printers
WIN-Q4788GPE9L7 Backup Operators                          Backup Operators can override s
WIN-Q4788GPE9L7 Replicator                                Supports file replication in a
WIN-Q4788GPE9L7 Remote Desktop Users                      Members in this group are grant
WIN-Q4788GPE9L7 Network Configuration Operators           Members in this group can have
WIN-Q4788GPE9L7 Performance Monitor Users                 Members of this group can acces
WIN-Q4788GPE9L7 Performance Log Users                     Members of this group may sched
WIN-Q4788GPE9L7 Distributed COM Users                     Members are allowed to launch,
WIN-Q4788GPE9L7 IIS_IUSRS                                 Built-in group used by Internet
WIN-Q4788GPE9L7 Cryptographic Operators                   Members are authorized to perfo
WIN-Q4788GPE9L7 Event Log Readers                         Members of this group can read
WIN-Q4788GPE9L7 Certificate Service DCOM Access           Members of this group are allow
WIN-Q4788GPE9L7 RDS Remote Access Servers                 Servers in this group enable us
WIN-Q4788GPE9L7 RDS Endpoint Servers                      Servers in this group run virtu
WIN-Q4788GPE9L7 RDS Management Servers                    Servers in this group can perfo
WIN-Q4788GPE9L7 Hyper-V Administrators                    Members of this group have comp
WIN-Q4788GPE9L7 Access Control Assistance Operators       Members of this group can remot
WIN-Q4788GPE9L7 Remote Management Users                   Members of this group can acces
WIN-Q4788GPE9L7 Storage Replica Administrators            Members of this group have comp
WIN-Q4788GPE9L7 Cert Publishers                           Members of this group are permi
```

getting local groups with a little filter

```
Get-NetLocalGroup -ComputerName WIN-Q4788GPE9L7 |select groupname
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetLocalGroup -ComputerName WIN-Q4788GPE9L7 |select groupname

GroupName
---------
Server Operators
Account Operators
Pre-Windows 2000 Compatible Access
Incoming Forest Trust Builders
Windows Authorization Access Group
Terminal Server License Servers
Administrators
Users
Guests
Print Operators
Backup Operators
Replicator
Remote Desktop Users
Network Configuration Operators
Performance Monitor Users
Performance Log Users
Distributed COM Users
IIS_IUSRS
```

getting the active logged in users on the machine needs local administrative access on the target

```
Get-NetLoggedon -ComputerName DESKTOP-V0AN63P
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetLoggedon -ComputerName DESKTOP-V0AN63P


UserName      : rem01x
LogonDomain   : crtp
AuthDomains   :
LogonServer   : WIN-Q4788GPE9L7
ComputerName : DESKTOP-V0AN63P

UserName      : DESKTOP-V0AN63P$
LogonDomain   : crtp
AuthDomains   :
LogonServer   :
ComputerName : DESKTOP-V0AN63P

UserName      : DESKTOP-V0AN63P$
LogonDomain   : crtp
AuthDomains   :
LogonServer   :
ComputerName : DESKTOP-V0AN63P

UserName      : DESKTOP-V0AN63P$
LogonDomain   : crtp
AuthDomains   :
LogonServer   :
ComputerName : DESKTOP-V0AN63P
```

same command with little filter

```
Get-NetLoggedon -ComputerName DESKTOP-V0AN63P |select username
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetLoggedon -ComputerName DESKTOP-V0AN63P |select username

UserName
--------
rem01x
DESKTOP-V0AN63P$
DESKTOP-V0AN63P$
DESKTOP-V0AN63P$
DESKTOP-V0AN63P$
DESKTOP-V0AN63P$
```

getting locally logged on users requires remote registry on the target

```
Get-LoggedOnLocal -ComputerName DESKTOP-V0AN63P
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-LoggedOnLocal -ComputerName DESKTOP-V0AN63P
PS C:\Users\rem01x.crtp\Desktop\tools>
```

getting the last logged in user on the machine requires administrative access and remote registry

```
Get-LastLoggedOn -ComputerName DESKTOP-V0AN63P
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-LastLoggedOn -ComputerName DESKTOP-V0AN63P

ComputerName    LastLoggedOn
------------    ------------
DESKTOP-V0AN63P crtp\rem01x
```

finding shares on the hosts in current domain

```
Invoke-ShareFinder -Verbose
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Invoke-ShareFinder -Verbose
VERBOSE: [Find-DomainShare] Querying computers in the domain
VERBOSE: [Get-DomainSearcher] search base: LDAP://WIN-Q4788GPE9L7.CRTP.LOCAL/DC=CRTP,DC=LOCAL
VERBOSE: [Get-DomainComputer] Get-DomainComputer filter string: (&(samAccountType=805306369))
VERBOSE: [Find-DomainShare] TargetComputers length: 2
VERBOSE: [Find-DomainShare] Using threading with threads: 20
VERBOSE: [New-ThreadedFunction] Total number of hosts: 2
VERBOSE: [New-ThreadedFunction] Total number of threads/partitions: 2
VERBOSE: [New-ThreadedFunction] Threads executing
VERBOSE: [New-ThreadedFunction] Waiting 100 seconds for final cleanup...

VERBOSE: [New-ThreadedFunction] all threads completed
Name           Type Remark               ComputerName
----           ---- ------               ------------
ADMIN$    2147483648 Remote Admin        WIN-Q4788GPE9L7.crtp.local
C$        2147483648 Default share       WIN-Q4788GPE9L7.crtp.local
Common             0                     WIN-Q4788GPE9L7.crtp.local
IPC$      2147483651 Remote IPC          WIN-Q4788GPE9L7.crtp.local
NETLOGON           0 Logon server share  WIN-Q4788GPE9L7.crtp.local
SYSVOL             0 Logon server share  WIN-Q4788GPE9L7.crtp.local
ADMIN$    2147483648 Remote Admin        DESKTOP-V0AN63P.crtp.local
C$        2147483648 Default share       DESKTOP-V0AN63P.crtp.local
IPC$      2147483651 Remote IPC          DESKTOP-V0AN63P.crtp.local
```

finding sensitive files on computers in the domain

```
Invoke-FileFinder -Verbose
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Invoke-FileFinder -Verbose
VERBOSE: [Find-InterestingDomainShareFile] Querying computers in the domain
VERBOSE: [Get-DomainSearcher] search base: LDAP://WIN-Q4788GPE9L7.CRTP.LOCAL/DC=CRTP,DC=LOCAL
VERBOSE: [Get-DomainComputer] Get-DomainComputer filter string: (&(samAccountType=805306369))
VERBOSE: [Find-InterestingDomainShareFile] TargetComputers length: 2
VERBOSE: [Find-InterestingDomainShareFile] Using threading with threads: 20
VERBOSE: [New-ThreadedFunction] Total number of hosts: 2
VERBOSE: [New-ThreadedFunction] Total number of threads/partitions: 2
VERBOSE: [New-ThreadedFunction] Threads executing
VERBOSE: [New-ThreadedFunction] Waiting 100 seconds for final cleanup...
VERBOSE: [New-ThreadedFunction] all threads completed
```

we don't have sensitive files here 😅

getting all file servers in the domain

```
Get-NetFileServer -Verbose
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetFileServer -Verbose
VERBOSE: [Get-DomainSearcher] search base: LDAP://WIN-Q4788GPE9L7.CRTP.LOCAL/DC=CRTP,DC=LOCAL
PS C:\Users\rem01x.crtp\Desktop\tools>
```

getting information about group policy

```
Get-NetGPO
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGPO

usncreated                : 5672
systemflags               : -1946157056
displayname               : Default Domain Policy
gpcmachineextensionnames  : [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{53D6AB1
                            9E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-1
                            11D2-A4EA-00C04F79F83A}{53D6AB1B-2488-11D1-A28C
whenchanged               : 10/14/2023 9:05:26 PM
objectclass               : {top, container, groupPolicyContainer}
gpcfunctionalityversion   : 2
showinadvancedviewonly    : True
usnchanged                : 16624
dscorepropagationdata     : {10/14/2023 8:47:00 PM, 1/1/1601 12:00:00 AM}
name                      : {31B2F340-016D-11D2-945F-00C04FB984F9}
flags                     : 0
cn                        : {31B2F340-016D-11D2-945F-00C04FB984F9}
iscriticalsystemobject    : True
```

getting information about group policy for another computer

```
Get-NetGPO -ComputerName WIN-Q4788GPE9L7
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGPO -ComputerName WIN-Q4788GPE9L7


usncreated                : 5675
systemflags               : -1946157056
displayname               : Default Domain Controllers Policy
gpcmachineextensionnames  : [{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}]
whenchanged               : 10/14/2023 8:46:05 PM
objectclass               : {top, container, groupPolicyContainer}
gpcfunctionalityversion   : 2
showinadvancedviewonly    : True
usnchanged                : 5675
dscorepropagationdata     : {10/14/2023 8:47:00 PM, 1/1/1601 12:00:00 AM}
name                      : {6AC1786C-016F-11D2-945F-00C04fB984F9}
flags                     : 0
cn                        : {6AC1786C-016F-11D2-945F-00C04fB984F9}
iscriticalsystemobject    : True
gpcfilesyspath            : \\crtp.local\sysvol\crtp.local\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}
distinguishedname         : CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=crtp,DC=local
whencreated               : 10/14/2023 8:46:05 PM
versionnumber             : 1
instancetype              : 4
objectguid                : 464079e4-19ee-4029-acde-3a614497c62d
objectcategory            : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=crtp,DC=local
```

getting filtered name

```
Get-NetGPO | select displayname
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGPO |select displayname

displayname
-----------
Default Domain Policy
Default Domain Controllers Policy
Disable Windows Defender
```

getting information about restricted group policy

```
Get-NetGPOGroup
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGPOGroup
PS C:\Users\rem01x.crtp\Desktop\tools>
```

as we see we didn’t get any because there is no misconfiguration for this

getting information about users which are part of local group using group policy

```
Find-GPOComputerAdmin -ComputerName WIN-Q4788GPE9L7
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Find-GPOComputerAdmin -ComputerName WIN-Q4788GPE9L7
PS C:\Users\rem01x.crtp\Desktop\tools>
```

we didn't find any for this but it may be a good hit

finding the machines where the user is a part of a specific group

```
Find-GPOLocation rem01x -Verbose
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Find-GPOLocation rem01x -Verbose
VERBOSE: [Get-DomainSearcher] search base: LDAP://WIN-Q4788GPE9L7.CRTP.LOCAL/DC=CRTP,DC=LOCAL
VERBOSE: [Get-DomainObject] Get-DomainObject filter string:
(&(|(|(samAccountName=rem01x)(name=rem01x)(displayname=rem01x))))
VERBOSE: [Get-DomainGPOUserLocalGroupMapping] Enumerating nested group memberships for:
'S-1-5-21-701016945-1456686922-2798200677-1455'
VERBOSE: [Get-DomainSearcher] search base: LDAP://WIN-Q4788GPE9L7.CRTP.LOCAL/DC=CRTP,DC=LOCAL
VERBOSE: [Get-DomainSearcher] search base: LDAP://WIN-Q4788GPE9L7.CRTP.LOCAL/DC=CRTP,DC=LOCAL
VERBOSE: [Get-DomainObject] Get-DomainObject filter string:
(&(|(objectsid=S-1-5-21-701016945-1456686922-2798200677-1455)))
VERBOSE: [Get-DomainSearcher] search base: LDAP://WIN-Q4788GPE9L7.CRTP.LOCAL/DC=CRTP,DC=LOCAL
VERBOSE: [Get-DomainObject] Get-DomainObject filter string:
(&(|(objectsid=S-1-5-21-701016945-1456686922-2798200677-513)))
VERBOSE: [Get-DomainGPOUserLocalGroupMapping] Target localgroup SID: S-1-5-32-544
VERBOSE: [Get-DomainGPOUserLocalGroupMapping] Effective target domain SIDs:
S-1-5-21-701016945-1456686922-2798200677-1455 S-1-5-21-701016945-1456686922-2798200677-513
VERBOSE: [Get-DomainSearcher] search base: LDAP://WIN-Q4788GPE9L7.CRTP.LOCAL/DC=CRTP,DC=LOCAL
VERBOSE: [Get-DomainGPO] filter string: (&(objectCategory=groupPolicyContainer))
VERBOSE: [Get-GptTmpl] Parsing GptTmplPath:
```

getting information about the Organizational Units OU

```
Get-NetOU -Verbose
```

getting information about acl

```
Get-ObjectAcl -Name rem01x -ResolveGUIDs
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-ObjectAcl -Name rem01x -ResolveGUIDs

AceQualifier           : AccessAllowed
ObjectDN               : CN=rem01x,CN=Users,DC=crtp,DC=local
ActiveDirectoryRights  : ReadProperty
ObjectAceType          : User-Account-Restrictions
ObjectSID              : S-1-5-21-701016945-1456686922-2798200677-1455
InheritanceFlags       : None
BinaryLength           : 56
AceType                : AccessAllowedObject
ObjectAceFlags         : ObjectAceTypePresent
IsCallback             : False
PropagationFlags       : None
SecurityIdentifier     : S-1-5-21-701016945-1456686922-2798200677-553
AccessMask             : 16
AuditFlags             : None
IsInherited            : False
AceFlags               : None
InheritedObjectAceType : All
OpaqueLength           : 0
```

now applying some filters

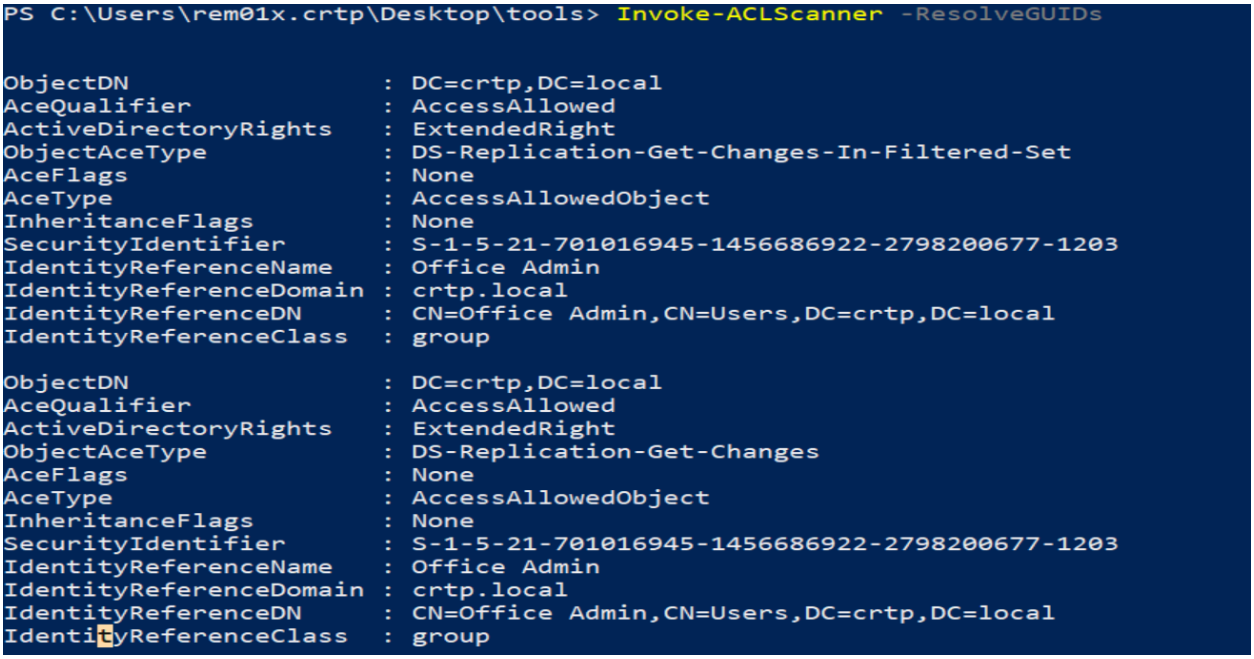
```
Get-ObjectAcl -Name rem01x -ResolveGUIDs | select ObjectDN,AceType,ActiveDirectoryRights,InheritanceFlags,IsInherited
```

```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-ObjectAcl -Name rem01x -ResolveGUIDs | select AceType,ActiveDirectoryRights,InheritanceFlags,IsInherited

          AceType                                                ActiveDirectoryRights InheritanceFlags IsInherited
          -------                                                --------------------- ---------------- -----------
AccessAllowedObject                                                        ReadProperty             None       False
AccessAllowedObject                                                        ReadProperty             None       False
AccessAllowedObject                                                        ReadProperty             None       False
AccessAllowedObject                                                        ReadProperty             None       False
AccessAllowedObject                                     ReadProperty, WriteProperty             None       False
AccessAllowedObject                                                      ReadProperty              None       False
AccessAllowedObject                                     ReadProperty, WriteProperty             None       False
AccessAllowedObject                                     ReadProperty, WriteProperty             None       False
AccessAllowedObject                                                     ExtendedRight            None       False
AccessAllowedObject                                                     ExtendedRight            None       False
AccessAllowedObject                                                     ExtendedRight            None       False
AccessAllowedObject                                                     ExtendedRight            None       False
AccessAllowedObject                                                        ReadProperty             None       False
AccessAllowedObject                                                        ReadProperty             None       False
AccessAllowedObject                                                        ReadProperty             None       False
AccessAllowedObject                                                        ReadProperty             None       False
AccessAllowedObject                                     ReadProperty, WriteProperty             None       False
AccessAllowedObject                                     ReadProperty, WriteProperty             None       False
AccessAllowedObject                                     ReadProperty, WriteProperty             None       False
     AccessAllowed                                                       GenericAll            None       False
     AccessAllowed                                                       GenericAll            None       False
     AccessAllowed                                                      ReadControl            None       False
     AccessAllowed                                                     GenericRead             None       False
     AccessAllowed                                                      GenericAll             None       False
```

getting information about interesting aces

```
Invoke-ACLScanner -ResolveGUIDs
```


PS C:\Users\rem01x.crtp\Desktop\tools> Invoke-ACLScanner -ResolveGUIDs
ObjectDN : DC=crtp,DC=local
AceQualifier : AccessAllowed
ActiveDirectoryRights : ExtendedRight
ObjectAceType : DS-Replication-Get-Changes-In-Filtered-Set
AceFlags : None
AceType : AccessAllowedObject
InheritanceFlags : None
SecurityIdentifier : S-1-5-21-701016945-1456686922-2798200677-1203
IdentityReferenceName : Office Admin
IdentityReferenceDomain : crtp.local
IdentityReferenceDN : CN=Office Admin,CN=Users,DC=crtp,DC=local
IdentityReferenceClass : group
ObjectDN : DC=crtp,DC=local
AceQualifier : AccessAllowed
ActiveDirectoryRights : ExtendedRight
ObjectAceType : DS-Replication-Get-Changes
AceFlags : None
AceType : AccessAllowedObject
InheritanceFlags : None
SecurityIdentifier : S-1-5-21-701016945-1456686922-2798200677-1203
IdentityReferenceName : Office Admin
IdentityReferenceDomain : crtp.local
IdentityReferenceDN : CN=Office Admin,CN=Users,DC=crtp,DC=local
IdentityReferenceClass : group