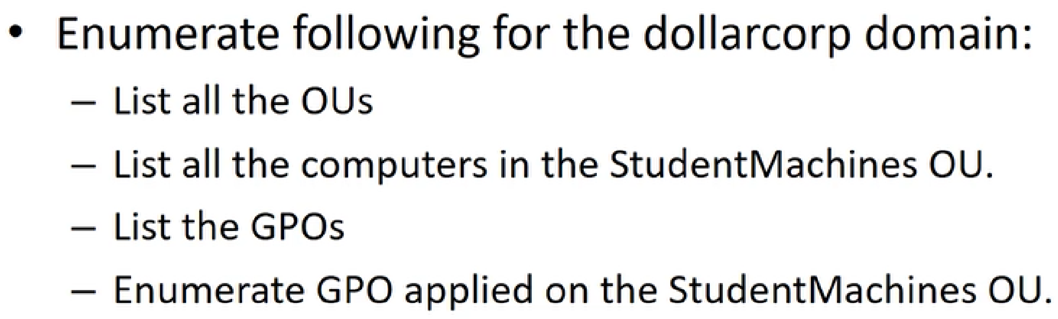
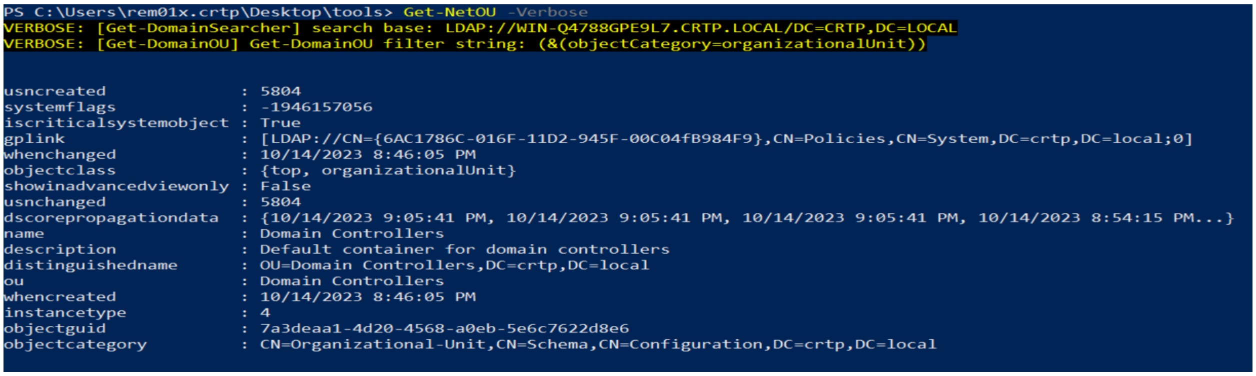
Learning Objective 2



- Enumerate following for the dollarcorp domain:
  - List all the OUs
  - List all the computers in the StudentMachines OU.
  - List the GPOs
  - Enumerate GPO applied on the StudentMachines OU.

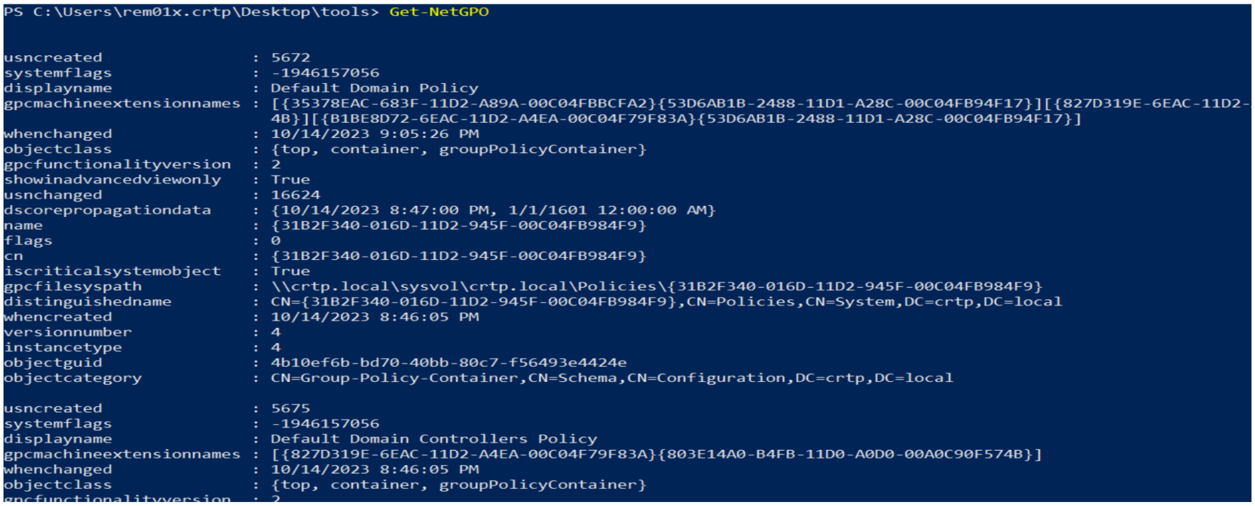
```
Get-NetOU -Verbose
```



```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetOU -Verbose
VERBOSE: [Get-DomainSearcher] search base: LDAP://WIN-Q4788GPE9L7.CRTP.LOCAL/DC=CRTP,DC=LOCAL
VERBOSE: [Get-DomainOU] Get-DomainOU filter string: (&(objectCategory=organizationalUnit))


usncreated              : 5804
systemflags             : -1946157056
iscriticalsystemobject  : True
gplink                  : [LDAP://CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=crtp,DC=local;0]
whenchanged             : 10/14/2023 8:46:05 PM
objectclass             : {top, organizationalUnit}
showinadvancedviewonly  : False
usnchanged              : 5804
dscorepropagationdata   : {10/14/2023 9:05:41 PM, 10/14/2023 9:05:41 PM, 10/14/2023 9:05:41 PM, 10/14/2023 8:54:15 PM...}
name                    : Domain Controllers
description             : Default container for domain controllers
distinguishedname       : OU=Domain Controllers,DC=crtp,DC=local
ou                      : Domain Controllers
whencreated             : 10/14/2023 8:46:05 PM
instancetype            : 4
objectguid              : 7a3deaa1-4d20-4568-a0eb-5e6c7622d8e6
objectcategory          : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=crtp,DC=local
```

```
Get-NetGPO
```



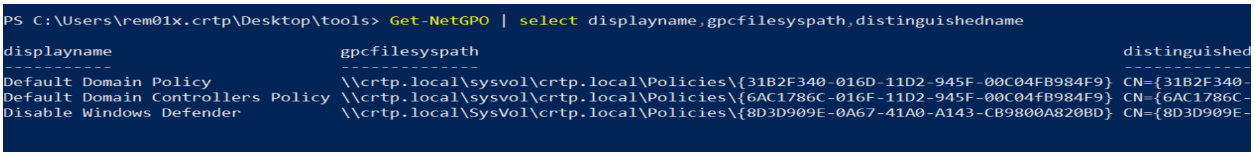
```
PS C:\Users\rem01x.crtp\Desktop\tools> Get-NetGPO


usncreated                 : 5672
systemflags                : -1946157056
displayname                : Default Domain Policy
gpcmachineextensionnames : [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}][{827D319E-6EAC-11D2-
                             4B}][{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}]
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
gpcfilesyspath             : \\crtp.local\sysvol\crtp.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
distinguishedname          : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=crtp,DC=local
whencreated                : 10/14/2023 8:46:05 PM
versionnumber              : 4
instancetype               : 4
objectguid                 : 4b10ef6b-bd70-40bb-80c7-f56493e4424e
objectcategory             : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=crtp,DC=local

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
```

some filters

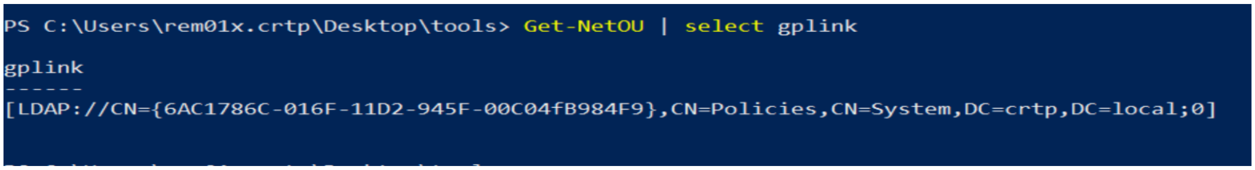
```
Get-NetGPO | select displayname,gpcfilesyspath,distinguishedname
```



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

displayname                       gpcfilesyspath                                                              distinguished
-----------                       --------------                                                              -------------
Default Domain Policy             \\crtp.local\sysvol\crtp.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9} CN={31B2F340-
Default Domain Controllers Policy \\crtp.local\sysvol\crtp.local\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9} CN={6AC1786C-
Disable Windows Defender          \\crtp.local\SysVol\crtp.local\Policies\{8D3D909E-0A67-41A0-A143-CB9800A820BD} CN={8D3D909E-
```

```
Get-NetOU | select gplink
```



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

gplink
------
[LDAP://CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=crtp,DC=local;0]
```