# Learning objective 1

## Powerview

Get all user in the domain

```
PS C:\ad> Get-NetUser | select samaccountname,userprincipalname

samaccountname userprincipalname
-------------- -----------------
Administrator
Guest
krbtgt
student141     student141@dollarcorp.moneycorp.local
webadmin       webadmin@dollarcorp.moneycorp.local
svcadmin       svcadmin@dollarcorp.moneycorp.local
ciadmin        ciadmin@dollarcorp.moneycorp.local
sqladmin       sqladmin@dollarcorp.moneycorp.local
```

Get all computers in the domain

```
PS C:\ad> Get-NetComputer -FullData | select dnshostname, operatingsystem

dnshostname                         operatingsystem
-----------                         ---------------
dcorp-dc.dollarcorp.moneycorp.local Windows Server 2019 Standard
WEB.dollarcorp.moneycorp.local      Windows 7 Enterprise
CI.dollarcorp.moneycorp.local       Windows 10 Education N
red.dollarcorp.moneycorp.local      Windows 10 Education
SQL.dollarcorp.moneycorp.local      Windows Server 2019 Standard
```

Get all domain admin

```
PS C:\ad> Get-NetGroupMember -GroupName "domain admins" | select groupdomain, groupname,
membername

GroupDomain                GroupName     MemberName
-----------                ---------     ----------
dollarcorp.moneycorp.local Domain Admins svcadmin
dollarcorp.moneycorp.local Domain Admins Administrator
```

Get enterprise admins

```
PS C:\ad> Get-NetGroupMember -groupname "enterprise*" -domain moneycorp.local | select
groupdomain,groupname,membername

GroupDomain     GroupName         MemberName
-----------     ---------         ----------
moneycorp.local Enterprise Admins Administrator
```

Get interesting shares

```
PS C:\ad> invoke-sharefinder -Verbose
VERBOSE: [*] Running Invoke-ShareFinder with delay of 0
VERBOSE: [*] Querying domain dollarcorp.moneycorp.local for hosts
VERBOSE: Get-DomainSearcher search string: LDAP://dcorp-
dc.dollarcorp.moneycorp.local/DC=dollarcorp,DC=moneycorp,DC=local
VERBOSE: Get-NetComputer filter : '(&(sAMAccountType=805306369)(dnshostname=*))'
VERBOSE: [*] Total number of hosts: 5
VERBOSE: Waiting for threads to finish...
WEB.dollarcorp.moneycorp.local
VERBOSE: All threads completed!
VERBOSE: [*] Total number of active hosts: 5
VERBOSE: [*] Enumerating server CI.dollarcorp.moneycorp.local (4 of 5)
```

```
VERBOSE: [*] Server share: @{shi1_netname=ADMIN$; shi1_type=2147483648; shi1_remark=Remote
Admin; ComputerName=CI.dollarcorp.moneycorp.local}
VERBOSE: [*] Server share: @{shi1_netname=C$; shi1_type=2147483648; shi1_remark=Default share;
ComputerName=CI.dollarcorp.moneycorp.local}
VERBOSE: [*] Server share: @{shi1_netname=IPC$; shi1_type=2147483651; shi1_remark=Remote IPC;
ComputerName=CI.dollarcorp.moneycorp.local}
VERBOSE: [*] Server share: @{shi1_netname=MyShare; shi1_type=0; shi1_remark=;
ComputerName=CI.dollarcorp.moneycorp.local}
VERBOSE: [*] Enumerating server WEB.dollarcorp.moneycorp.local (5 of 5)
VERBOSE: [*] Server share: @{shi1_netname=ADMIN$; shi1_type=2147483648; shi1_remark=Remote
Admin; ComputerName=WEB.dollarcorp.moneycorp.local}
VERBOSE: [*] Server share: @{shi1_netname=C$; shi1_type=2147483648; shi1_remark=Default share;
ComputerName=WEB.dollarcorp.moneycorp.local}
VERBOSE: [*] Server share: @{shi1_netname=IPC$; shi1_type=2147483651; shi1_remark=Remote IPC;
ComputerName=WEB.dollarcorp.moneycorp.local}
VERBOSE: [*] Server share: @{shi1_netname=myshare; shi1_type=0; shi1_remark=;
ComputerName=WEB.dollarcorp.moneycorp.local}
VERBOSE: [*] Server share: @{shi1_netname=Users; shi1_type=0; shi1_remark=;
ComputerName=WEB.dollarcorp.moneycorp.local}
```

## Ad module

Get all users in the domain

```
PS C:\ad\ADModule-master\ActiveDirectory> Get-ADUser -Filter * | select
samaccountname,userprincipalname

samaccountname userprincipalname
-------------- -----------------
Administrator
Guest
krbtgt
student141     student141@dollarcorp.moneycorp.local
MONEYCORP$
webadmin       webadmin@dollarcorp.moneycorp.local
svcadmin       svcadmin@dollarcorp.moneycorp.local
ciadmin        ciadmin@dollarcorp.moneycorp.local
sqladmin       sqladmin@dollarcorp.moneycorp.local
```

Get all computers in the domain

```
PS C:\ad\ADModule-master\ActiveDirectory> Get-ADComputer -Filter * | select
dnshostname,samaccountname

dnshostname                        samaccountname
-----------                        --------------
dcorp-dc.dollarcorp.moneycorp.local DCORP-DC$
WEB.dollarcorp.moneycorp.local      WEB$
CI.dollarcorp.moneycorp.local       CI$
red.dollarcorp.moneycorp.local      RED$
SQL.dollarcorp.moneycorp.local      SQL$
```

Get all domain admin

```
PS C:\ad\ADModule-master\ActiveDirectory> Get-ADGroupMember -Identity "domain admins" -
Recursive|select samaccountname,distinguishedname,sid

samaccountname distinguishedname                                        sid
-------------- -----------------                                        ---
Administrator  CN=Administrator,CN=Users,DC=dollarcorp,DC=moneycorp,DC=local S-1-5-21-
2255310023-4090572302-666251596-500
svcadmin       CN=svcadmin,OU=DCORPUSERS,DC=dollarcorp,DC=moneycorp,DC=local S-1-5-21-
2255310023-4090572302-666251596-1107
```

Get enterprise admin

```
PS C:\ad\ADModule-master\ActiveDirectory> Get-ADGroupMember -Identity "domain admins" -Server
moneycorp.local -Recursive|select samaccountname,distinguishedname,sid
```

```
samaccountname distinguishedname                              sid
-------------- -----------------                              ---
Administrator  CN=Administrator,CN=Users,DC=moneycorp,DC=local S-1-5-21-2548476665-130003349-
940611390-500
```