**PED Preparation**

Example will be given for one forest with two domains:

**oodba.com** and **sector.oodba.com**

Prepare Tier0\_Users.csv file. This file can contain users from whole forest. Users must be defined by the DistinguishedName and header should be “DN”. Copy this file to the root domain together with GetUserInfoDN.ps1 script.

Graphical user interface, text

Description automatically generated

Run *GetUserInfoDN.ps1* against *Tier0\_Users.csv*

A screenshot of a computer

Description automatically generated with low confidence

2 CSV files per domain will be created.

Text

Description automatically generated

* Users: Tier0\_Accs\_domain.name.csv

Graphical user interface

Description automatically generated

* Group membership: Tier0\_Grp\_Membership\_domain.name.csv

Text

Description automatically generated

Now, you need to populate PEDAction parameter for every user in Users file.

* Possible PED actions are:
  + Delete
  + Disable
  + Recreate
  + Reset
  + Deprivilege
  + Rename (you need to provide new name)
  + Create

Actions defined:

A screenshot of a computer

Description automatically generated with low confidence

Copy these files to the new folder on your machine. You need to have txt file with PED commands into same folder as Prepare\_CSVs.ps1. You will get one with Prepare\_CSVs.ps1 script. You can customize it for your needs.

Run Prepare\_CSVs.ps1 pointing to the folder with PED actions files. You will be asked to provide location for PED files:

Text

Description automatically generated

Result: PED folder with all scripts and CSVs for running PED gets created

Text

Description automatically generated

Note: By default, PED script will be downloaded directly from GitHub repository. If you are working offline, you can download this script from GitHub manually (https://github.com/oodbash/CR-Scripts-CB.git), and copy ZIP file to your workstation. Then, you should run Prepare\_CSVs.ps1 with following parameter:

.\prepare-csvs.ps1 -RawCSVsLocation "d:\lab" **-ScriptsLocation** "D:\LAB\CR-Scripts-CB-main.zip"

Optionally, define Reboot Plan in the CSV folder: “\_reboot\_plan.csv”

Copy PED folder to the root of PDC emulator

**PED Execution**

**Create temporary PED EA/DA Admin accounts**

Accounts to be created must be defined in the “\_temp\_admins\_to\_be\_created.csv” file in the CSV folder. Make sure the Organizational Unit exists! Otherwise, change it to the correct one!

Text

Description automatically generated

By default, the temporary accounts are member of the following groups. This is defined in “\_temp\_admins\_grp\_membership.csv”

Text

Description automatically generated

Run CreateUsers.ps1 to create the temporary admin accounts

Text

Description automatically generated

Copy the file “New\_accounts.csv” in the Scripts folder to the CSV folder and name it as follows: “oodba\_temp\_admins.csv”



Grant EA/DA admin rights to temporary admin accounts



Enforce replication:

repadmin /syncall /AdeP

**Disable old Tier 0 Admin accounts** (to be replaced with new Tier 0 accounts later)

.\DisableUsers.ps1 -csv ..\CSVs\oodba\_will\_be\_permanently\_disabled.csv

.\DisableUsers.ps1 -csv ..\CSVs\oodba\_will\_be\_renamed.csv

.\DisableUsers.ps1 -csv ..\CSVs\oodba\_will\_be\_recreated.csv -rename

Text

Description automatically generated

A new OU gets created under domain root level: “OU=CR Disabled Accounts”.

The accounts defined in the csv files specified above, get disabled and moved to the newly created OU. However, they still have high-privilege group memberships.

Graphical user interface, text, application

Description automatically generated

**Disable old Admin accounts** (which have password reset later)

import-csv ..\CSVs\oodba\_reset\_pass.csv | %{set-aduser $\_.name -Enabled:$false}



**Deprivilege users**

**.\deprivilegeusers.ps1 -CSV C:\ped\CSVs\oodba\_will\_be\_removed\_from\_tier\_0.csv -tier0 -move**

**Graphical user interface, text, application

Description automatically generated**

**KRBTGT Reset**

Execute First Kerberos Reset:

.\New-CtmADKrbtgtKeys.ps1

### WAIT! ###

Execute Second Kerberos Reset:

.\New-CtmADKrbtgtKeys.ps1

Restart All DCs according to Reboot plan.

.\RemoteServerRestart.ps1 -CSV ..\CSVs\oodba\_reboot\_plan.csv

**Create and new Tier 0 admin accounts and issue passwords to administrators**

Make sure the OrganizationUnit is correct.

Text

Description automatically generated

.\CreateUsers.ps1 -csv ..\CSVs\oodba\_new\_admins\_to\_be\_created.csv

Text

Description automatically generated

Both accounts are created in the Tier 0 OU.

Copy the file “New\_accounts.csv” in the Scripts folder to the CSV folder and name it as follows: “oodba\_new\_admins.csv”

 Grant Tier 0 Admin rights to new accounts

If the OUs, or groups are named differently, make sure to modify it in the “MakeItTier0.ps1” Script:

Graphical user interface, text, application

Description automatically generated



New accounts get added to the Tier0Admins group

Configure new Tier 0 accounts as "account sensitive and can't be delegated"

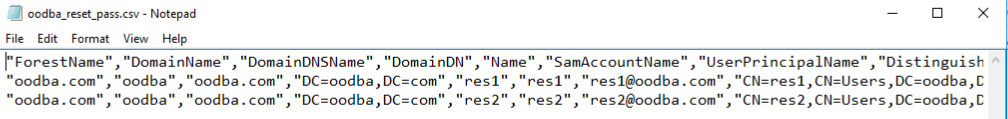
import-csv ..\CSVs\oodba\_new\_admins.csv | %{set-aduser $\_.samaccountname -AccountNotDelegated:$true}



Grant admin rights to temporary admin accounts



**Reset passwords on defined accounts:**



.\ResetPasswordsFromFile.ps1 -csv ..\CSVs\oodba\_reset\_pass.csv -showpass



Copy the file “New\_Passwords.csv” in the Scripts folder to the CSV folder and name it as follows: “oodba\_pwdreset\_new\_admins.csv”

Copy-Item .\New\_Passwords.csv ..\CSVs\oodba\_pwdreset\_new\_admins.csv



Graphical user interface, text, application

Description automatically generated

Enable accounts which had their password reset

import-csv ..\CSVs\oodba\_reset\_pass.csv | %{set-aduser $\_.name -Enabled:$true}



**Cleanup / Remove all temporary accounts and permissions**

.\DeleteUsers.ps1 -csv ..\CSVs\oodba\_temp\_admins.csv Graphical user interface, text, application

Description automatically generated