**Useful PowerView function:**

**Copy-ClonedFile** - copies a local file to a remote location, matching MAC properties.

**Find-InterestingFile** -search a local or remote path for files with specific terms in the name.

**Get-LastLoggedOn** - return the last logged on user for a target host.

**Find-GPOComputerAdmin** - takes a computer and determines who has admin rights over it through GPO enumeration.

**Get-DomainPolicy** - returns the default domain or DC policy.

**Invoke-UserHunter -** finds machines on the local domain where specified users are logged into, and can optionally check if the current user has local admin access to found machines.

**Invoke-StealthUserHunter** - finds all file servers utilizes in user HomeDirectories, and checks the sessions one each file server, hunting for particular users.

**Domain Trust Functions – I found all 5 of them useful.**

**Invoke-FileFinder** - finds potentially sensitive files on hosts in the local domain.

**Find-ManagedSecurityGroups** - searches for active directory security groups which are managed and identify users who have writing access.

**Get-ExploitableSystem** - finds systems likely vulnerable to common exploits.

**DSQUERY/DSGET useful functions:**find all members **for a particular group**   
- dsget group "<DN of the group>" -members.  
**How to find Domain Naming Master in a Forest –**  
 dsquery server -forest -hasfsmo Name.  
**List of all users with primary group "Domain Users"** -  
dsquery \* -filter "(primaryGroupID=513)" -limit 0

**Export all usernames and email addresses** - dsquery.exe \* -limit 0 -filter "(&(objectCategory=person)(objectClass=user)(mail=\*))" -attr sAMAccountName name mail >"c:\PrimaryEmailAddresses.txt"  
**Stale computer/user accounts** - dsquery computer/user domainroot -stalepwd 180 -limit 0