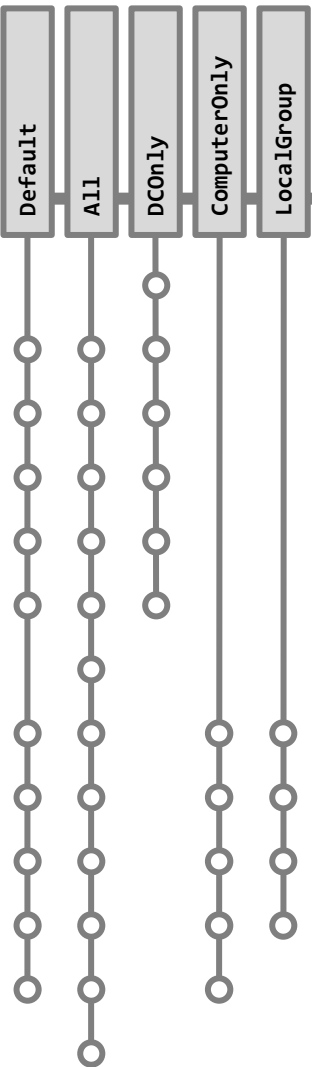


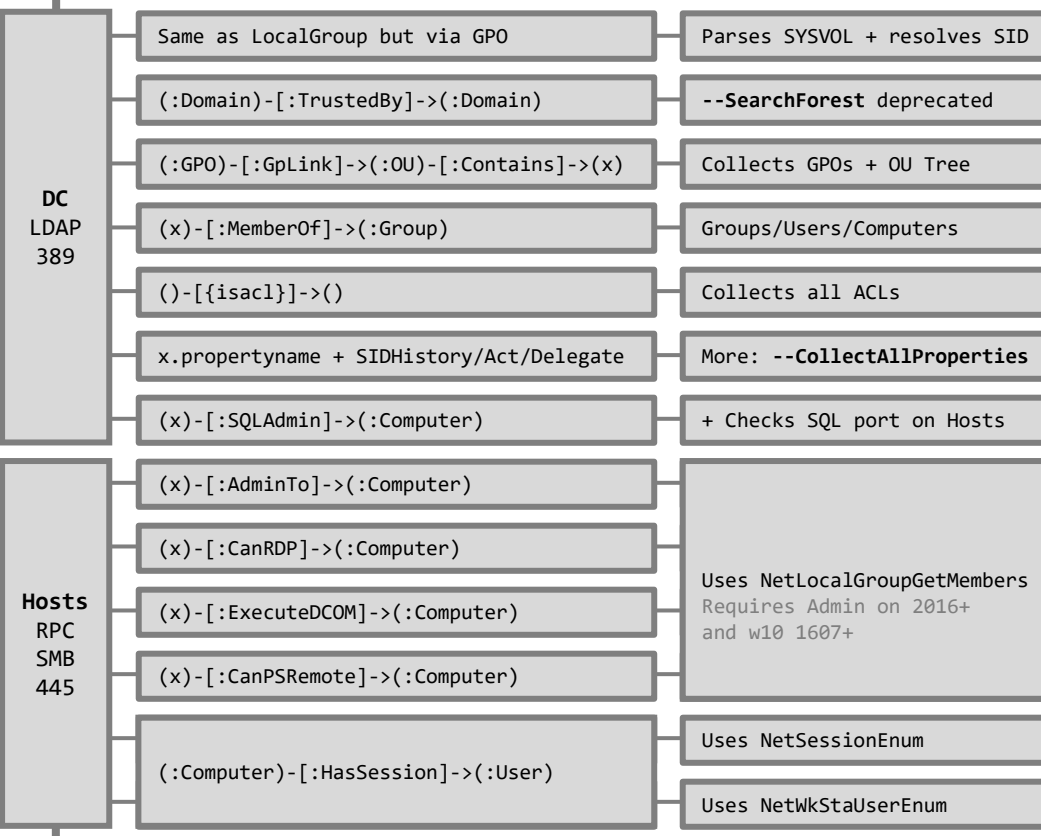
Sharphound.exe [--CollectionMethod <method[]>] [--Domain <domain[]>] [+]



- ### Collection Methods
- GPOLocalGroup
 - Trusts
 - Container
 - Group
 - ACL
 - ObjectProps
 - SPNTargets
 - LocalAdmin
 - RDP
 - DCOM
 - PSRemote
 - Session
 - LoggedOn

- Use **--LDAPFilter** to collect specific OU/Object [precision+/stealth+]
- Use **--SecureLDAP** to connect over LDAPS 636 iso LDAP 389 [Use **--LDAPPort** if other]
- Using **--Stealth** has no effect on DC methods

v0.0w
@SadProcessor



ATT&CK
S0521
TA0007

T1482

T1033
T1069.002
T1082
T1087.002

T1033
T1049
T1069.001
T1087.001
T1135

- Add **--Throttle** and **--Jitter** [stealth+]

Session vs LoggedOn:
 - **LoggedOn** is more accurate but requires Admin
 - **Session** requires Admin on 2016+ / w10 1607+
 - Using **--Stealth** on session methods will only target potentially interesting hosts

- Host methods also LDAP to DC for Host list and to resolve collected SIDs
- Use **--ComputerList** to bypass LDAPFilter
- Using **--Stealth** on LocalGroup methods reverts to GPOLocalGroup [DC]

- Use **--Loop** to increase session data coverage [attack paths nbr]
- Syntax: **-c session --Loop --LoopDuration** HH:MM:SS **--LoopInterval** HH:MM:SS
- Drop zips in UI to import > Will add new without erasing old



[Output: --ZipFileName / --OutputPrefix / --OutputDirectory / --RandomizeFileNames / --CacheFileName / ...] +more