rpcclient

```
# Anonymous connection (-N=no pass)
rpcclient -U “” -N <ip>

# Connection with user
rpcclient -U “user” <ip>

# Get information about the DC
srvinfo

# Get information about objects such as groups (enum*)
enumdomains
enumdomgroups
enumalsgroups builtin

# Try to get domain password policy
getdompwinfo

# Try to enumerate different truste domains
dsr_enumtrustdom

# Get username for a defined user ?
getusername

# Query user, group etc informations
queryuser RID
querygroupmem519
queryaliasmem builtin 0x220

# Query info policy
lsaquery

# Convert SID to names
lookupsids SID
```

enum4linux

```
# Verbose mode
enum4linux -v target-ip

# Do everything
enum4linux -a target-ip

# List users
enum4linux -U target-ip

# If you've managed to obtain credentials, you can pull a full list of users regardless of the RestrictAnonymous option
enum4linux -u administrator -p password -U target-ip
```

Get username from the defaut RID range (500-550, 1000-1050)
enum4linux -r target-ip

Get username using a custom RID range
enum4linux -R 600-660 target-ip

List groups
enum4linux -G target-ip

List shares
enum4linux -S target-ip

Perform a dictionary attack, if the server doesn't let you retrieve a share list
enum4linux -s shares.txt target-ip

Pulls OS information using smbclient, this can pull the service pack version on some versions of Windows
enum4linux -o target-ip

Pull information about printers known to the remove device.
enum4linux -i target-ip
enum4linux-ng is a rewrite of the official tool (python3)
adding some features like colors and parsing
https://github.com/cddmp/enum4linux-ng