SMB

SMB poking for open shares :

smbmap : can ommit username and password for anonymous login

smbmap -H 10.10.10.175 -u <username> -p <password>
smbmap -d <domain> -u <username> -p <password> -H 10.10.10.175 -R <directory>
smbmap -d egotistical-bank.local -u fsmith -p Thestrokes23 -H 10.10.10.175 -R Users
smbmap -H 10.10.10.100 -R <directory> -A <file> -q
smbmap -H 10.10.10.130 -u anonymous --depth 5   --> worked

nmap

nmap --scripts safe -p 445 10.10.10.100

smbclient

smbclient //ip/share -U   --> smb shell
smbclient -L \\\\ ip\\ -U username   --> enumerate shares

smbclient -L //10.10.10.100
smbclient //10.10.10.100/Users
smbclient -N //10.10.10.130/batshare
smbclient -U anonymous //10.10.10.130/batshare
smbclient //HOST/PATH -c 'recurse;ls' PASS -U USER%PASSWORD

> recurse ON
> prompt OFF
> mget *

enum4linux : (does-not work very well)

enum4linux 10.10.10.100

msfconsole

use auxiliary/scanner/smb/smb_version

brute force a certain password on a list of users

hydra -L userlist -p 'Welcome123!' 10.10.10.169 smb