Basics:

help - Lists all commands.
cls - Clears screen
exit – Closes the CMD window.
cd – Change directory.
dir – Shows what's in a folder.
echo – Display text (great for scripts).
type filename.txt – Displays contents of a text file.
hostname – Shows your computer's name.
ver – See your Windows version.
color 0a – Makes CMD look like The Matrix.
taskkill /f /im explorer.exe – Kill desktop (and bring it back with start explorer.exe).

System Info:

systeminfo – Tells you everything about the system.
ipconfig – See your IP address and network config.
ipconfig /all – Order the whole menu.
getmac – Displays MAC addresses.
netstat – Shows active connections.
netstat -ano – Connections with PIDs.
tasklist – View running processes.
taskkill /PID [PID] /F – Kill a process.
whoami – Shows current user.
echo %username% – Another way to confirm user identity.
powercfg /batteryreport – Battery health report.

Network Diagnostics:

ping [IP/domain] – Check if a host is reachable.
tracert [domain] – Trace the path packets take.
nslookup [domain] – DNS lookup.
arp -a – Displays MAC to IP mapping.
netsh wlan show profiles – View saved Wi-Fi networks.
netsh wlan export profile [profile name] key=clear – Export Wi-Fi creds.
net view – Shows networked devices.
nbtstat -n – NetBIOS info.
net use – Map network drives.
net config workstation – Shows domain info.
sfc /scannow – Scan for system file corruption.

User Access:

net user – Shows all local users.
net user [username] – See info for a specific user.
net user [username] [password] /add – Add new user.
net localgroup administrators [username] /add – Make user an admin.
net accounts – Shows password policy.
whoami /groups – View security groups.
runas /user:domain\username cmd – Run as another user.
net localgroup – List local groups.
control userpasswords2 – GUI shortcut to user settings.
wmic useraccount list brief – Another way to list users.

File Directory & I/O

tree – See directory structure like a family tree.
attrib – View file attributes.
attrib +h [file] – Hide a file.
copy [file1] [file2] – Copy files.
move [file1] [folder] – Move files.
del [file] – Delete files.
ren [old] [new] – Rename files.
mkdir [folder] – Make a new directory.
rmdir [folder] – Remove a directory.
fc [file1] [file2] – Compare two files.
clip < [file] – Copy file contents to clipboard.

Security:

cipher /w:[drive] – Securely wipe deleted data.
secedit /export /cfg secconfig.cfg – Export local security policy.
wevtutil qe System /c:5 /f:text – View recent system logs.
wmic process list full – See detailed process info.
schtasks /query /fo LIST /v – View scheduled tasks.
dir /a – Show hidden and system files.
netsh advfirewall show allprofiles – See firewall settings.
auditpol /get /category:* – View audit policies.
reg query – Query the Windows registry (careful!).
findstr /i [text] [file] – Search for strings in files.

Malware Assessment:

wmic startup – Show startup programs.
netstat -b – See what's using network ports.
schtasks – See if malware is hiding in scheduled tasks.
tasklist /v – Detailed process info. Great for spotting weird stuff.
driverquery – Lists loaded drivers.
wmic service list brief – Spot rogue services.
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run – Startup registry keys.
dir /s /b – Recursively list all files. Helpful for finding hidden scripts.
type hosts – Look for DNS hijacks (C:\Windows\System32\drivers\etc\hosts).
sc query – Query services.

Automation:

echo off – Hides commands in batch files.
pause – Pauses a batch script.
goto – Moves to a label in script.
if exist – Conditional logic in scripts.
for /f – Loop through a file.
call – Call another batch file.
start – Launch programs from CMD.
rem – Add comments in scripts.
timeout /t 10 – Delay script for 10 seconds.
set – Set environment variables.

EXTRA!

wmic path softwarelicensingservice get OA3xOriginalProductKey – Get your Windows product key.
driverquery /v – More driver info.
ipconfig /flushdns – Clear DNS cache.
chkdsk – Check disk for errors.
assoc – File associations.
net user | find /i "admin" – See if any admin users exist.
netstat -an | find "443" – Look for HTTPS connections.
findstr /s /i "password" *.* – Find password strings in files.
net accounts /domain – Get domain password policy.
sc qc [service] – Get config of specific service.
powershell -command "[Net.Dns]::GetHostAddresses('domain.com')" – DNS lookup from CMD.
dir /s /b | findstr ".bat" – Find all .bat files recursively.
whoami /priv – See user privileges.
net group "Domain Admins" /domain – List domain admins (if you're on a domain).