Windows Cybersecurity Commands – Explained Reference

CMD – Files & Directories

```
dir                          # Lists files and folders in the current directory
mkdir nuevo                  # Creates a new directory named 'nuevo'
mkdir "%USERPROFILE%\Desktop\nuevo"   # Creates a folder on the user's Desktop
rmdir nuevo                  # Deletes an empty directory
rmdir /S /Q "%USERPROFILE%\Desktop\nuevo" # Deletes a directory and its contents
type nul > "%USERPROFILE%\Desktop\test.txt" # Creates an empty file
move "%USERPROFILE%\Downloads\bootcamp.txt" "%USERPROFILE%\Desktop" # Moves a file
del "%USERPROFILE%\Desktop\bootcamp.txt"    # Deletes a file
```

CMD – Text Handling

```
echo Estoy aprendiendo Ciberseguridad   # Prints text to the console
echo Ejercicio de pruebas > "%USERPROFILE%\Documents\test2.txt" # Creates file with content
echo Módulo 3 >> "%USERPROFILE%\Documents\test2.txt"             # Appends text to file
type "%USERPROFILE%\Documents\test2.txt"                          # Displays file contents
find "Ejercicio" "%USERPROFILE%\Documents\test2.txt"              # Searches text inside file
```

CMD – Processes

```
tasklist                     # Lists all running processes
tasklist | find "cmd.exe"    # Finds the PID of the CMD process
taskkill /PID 1234 /F        # Terminates a process by PID
```

CMD – Networking

```
ipconfig                     # Shows IP configuration
ipconfig /all                # Shows detailed network configuration
getmac                       # Displays MAC addresses
ping 127.0.0.1               # Tests local network stack (loopback)
nslookup google.com           # Performs DNS resolution
arp -a                       # Displays ARP cache
netstat -ano                 # Lists active connections and listening ports
tracert google.com            # Traces route to destination
```

CMD – Permissions

```
icacls "%USERPROFILE%\Desktop"          # Displays ACLs for Desktop
takeown /F C:\Windows\System32\cmd.exe # Attempts to take ownership of cmd.exe
```

PowerShell – Files & Directories

```
Get-ChildItem                               # Lists directory contents
New-Item -ItemType Directory -Path "$env:USERPROFILE\Desktop\nuevo" # Creates directory
New-Item -ItemType File -Path "$env:USERPROFILE\Desktop\test.txt"   # Creates empty file
Remove-Item "$env:USERPROFILE\Desktop\test.txt" -Force              # Deletes file
```

PowerShell – Text Handling

```
Write-Output "Estoy aprendiendo Ciberseguridad" # Prints text
Set-Content "$env:USERPROFILE\Documents\test2.txt" "Ejercicio de pruebas" # Writes file
Add-Content "$env:USERPROFILE\Documents\test2.txt" "Módulo 3"              # Appends text
Get-Content "$env:USERPROFILE\Documents\test2.txt"                         # Reads file
Select-String -Path "$env:USERPROFILE\Documents\test2.txt" -Pattern "Ejercicio" # Searches text
```

PowerShell – Processes

```
Get-Process                    # Lists running processes
Get-Process cmd                # Gets CMD process and PID
Stop-Process -Id 1234 -Force   # Terminates process by PID
```

PowerShell – Networking

```
Get-NetAdapter                  # Lists network adapters
Get-NetIPAddress                # Displays IP addresses
Get-NetIPConfiguration          # Shows full IP configuration
Test-NetConnection google.com  # Tests connectivity to host
```

PowerShell – Environment Variables

```
Get-ChildItem env:              # Lists environment variables
$env:var = "512"                # Creates a temporary environment variable
$env:MiRuta = "$env:USERPROFILE\Desktop" # Sets Desktop path as variable
Remove-Item env:var             # Deletes environment variable
```

PowerShell – Permissions

```
Get-Acl "$env:USERPROFILE\Desktop"       # Displays ACLs
Copy-Item "$env:USERPROFILE\Documents\admin.txt" "C:\Windows\System32" # Copies file as admin
Get-Acl "C:\Windows\System32\admin.txt" # Shows restrictive ACLs
```