

Microsoft Windows

Commandes réseau

ipconfig	Show network configuration
ipconfig /all	Detailed IP/DNS info for incident validation
ipconfig /release	Release IP to cut rogue connections
ipconfig /renew	Renew IP after network reset
ipconfig /flushdns	Clear DNS cache (stop DNS poisoning)
ping [IP]	Test host reachability (detect filtering/DoS)
tracert [IP]	Trace suspicious traffic path
nslookup [domain]	Investigate phishing/malware domains
netstat -an	Spot unusual open ports & connections
netstat -b	See which process is making network connections
arp -a	Detect ARP spoofing/poisoning attempts
hostname	Verify compromised system identity
getmac	Validate legitimate MAC addresses
net use	Check unauthorized shared drive access
net share	List shared resources for data exfil risks
net start	Spot suspicious or unauthorized services
net stop	Kill malicious services
tasklist	See running processes (correlate with netstat)
route print	Inspect routing table for anomalies
netsh advfirewall firewall show rule name=all	Review firewall rules for

From:
<https://www.adminsys.it/wiki/> - Admin Sys

Permanent link:
<https://www.adminsys.it/wiki/mswindows:start?rev=1757942505>

Last update: 2025/09/15 15:21

