

Microsoft Windows

Commandes réseau

- ipconfig /all - Show network configuration
- ipconfig /flushdns - 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 -o - Spot unusual open ports & connections
- netstat -b - See which process is making network connections
- arp -a - Detect ARP spoofing/poisoning attempts
- net user /add - Verify compromised system identity
- net user /delete - Validate legitimate MAC addresses
- net use - Check unauthorized shared drive access
- net share - List shared resources for data exfil risks
- net stop [service] - Spot suspicious or unauthorized services
- net kill [PID] - Kill malicious services
- tasklist - See running processes (correlate with netstat)
- netsh interface ipv4 show address - Inspect routing table for anomalies
- netsh advfirewall firewall show rule=... - Review firewall rules for

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

Permanent link:
<https://www.adminsys.it/wiki/mswindows:start?rev=1757940836>

Last update: **2025/09/15 14:53**

