Microsoft Windows

Commandes réseau

- □□□□□□□□ – Show network configuration
- □□□□□□□□ /□□□ – Detailed IP/DNS info for incident validation
- □□□□□□□□ /□□□□□□□ – Release IP to cut rogue connections
- □□□□□□□□ /□□□□□ – Renew IP after network reset
- □□□□□□□□ /□□□□□□□□ – Clear DNS cache (stop DNS poisoning)
- □□□□ [□□] – Test host reachability (detect filtering/DoS)
- □□□□□□□ [□□] – Trace suspicious traffic path
- □□□□□□□□ [□□□□□□] – Investigate phishing/malware domains
- □□□□□□□ -□□ – Spot unusual open ports & connections
- □□□□□□□ -□ – See which process is making network connections
- □□□ -□ – Detect ARP spoofing/poisoning attempts
- □□□□□□□□ – Verify compromised system identity
- □□□□□□ – Validate legitimate MAC addresses
- □□□ □□□ – Check unauthorized shared drive access
- □□□ □□□□□ – List shared resources for data exfil risks
- □□□ □□□□□ – Spot suspicious or unauthorized services
- □□□ □□□□ – Kill malicious services
- □□□□□□□□ – See running processes (correlate with netstat)
- □□□□□ □□□□□ – Inspect routing table for anomalies
- □□□□□ □□□□□□□□□□ □□□□□□□□ □□□□ □□□□ □□□□=□□□ – Review firewall rules for