CompTIA CySA+ (CS0-003) Commands Sheet

Practical commands for host triage, DNS checks, packet review, log analysis, and incident investigation.

Best for	Focus	Use with
Command recall before drills	What each command does and when to use it	Use with ports sheet and cheat sheet

1. Host and network triage

ipconfig /all	Check Windows addressing, DNS, and lease state.
ifconfig / ip a	Inspect interface settings on Unix-like systems.
ping	Test reachability and latency quickly.
tracert / traceroute	Map the path to a target.
arp -a	View local ARP cache entries.

2. DNS and connection checks

nslookup / dig	Query DNS records and test resolution.
netstat -ano	See active connections, listeners, and owning processes.
ss -tulpn	Linux socket and listener overview.
route print	Review local route table on Windows.
whois	Pull domain/registration context during investigations.

3. Packet and service investigation

tcpdump -i eth0	Capture packets on Linux.
Wireshark filters	Use protocol/address/field filters to isolate useful evidence.
curl -I URL	Quickly inspect HTTP headers and basic web responses.
openssl s_client	Inspect TLS handshake/certificate behavior.
nmap -sV	Service and version discovery.

4. Process and log review

tasklist / ps	List running processes.
taskkill / kill	Terminate a process if response requires it.
grep / findstr	Search text in files or command output.
journalctl	Query Linux logs.

Get-WinEvent	Query Windows event logs with filtering.

5. Analyst reminders

Correlate sources	One command output rarely proves root cause alone.
Preserve evidence	Do not destroy what you still need to analyze.
Document time	Timestamps matter in incident timelines.
Verify scope	After finding one bad host, check whether there are more.