CompTIA CASP+ (CAS-004) Commands Sheet

Practical commands and checks for enterprise validation, identity, crypto, networking, and secure operations. Legacy CAS-004 set.

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. Core validation

show logging / journalctl / Get-WinEvent	Logs are central to enterprise visibility and response.
show running-config	Confirm actual state before diagnosing architecture issues.
netstat / ss	Inspect sockets, listeners, and established sessions.
route print / ip route	Check host or network path logic.

2. Identity and crypto checks

whoami / id	Quick identity context on a host.
klist	Inspect Kerberos tickets on supported systems.
openssl s_client	Validate TLS handshakes and certificate chains.
certutil	Useful certificate-store and trust troubleshooting on Windows.

3. Network and service checks

nslookup / dig	Validate DNS answers and resolution paths.
ping / traceroute	Check basic reachability and path.
curl -I URL	Fast validation of web headers and responses.
tcpdump / Wireshark	Ground-truth packet visibility when theory is not enough.

4. Security operations checks

show access-lists	Validate policy logic and hit counts on network devices.
show aaa servers	Check AAA back-end visibility on supported devices.
show crypto ikev2 sa	Review VPN control-plane establishment.
show crypto ipsec sa	Check VPN data-plane counters and state.

5. Architect reminders

Correlate sources	Architecture decisions should be supported by logs, metrics, and operational evidence.
Validate rollback	A secure change still needs a safe recovery path.
Think integration	One command rarely answers the whole enterprise question.
Document decisions	Why a control was chosen matters for future operations and audits.