CompTIA Security+ (SY0-601) Commands Sheet

Practical commands for host, network, packet, and incident-response style questions.

Best for	Focus	Use with
Command recall before drills	What each command does and why it matters	Use with ports sheet and cheat sheet

1. Basic host investigation

ipconfig /all	Check Windows addressing, DNS, gateway, and lease state.
ifconfig / ip a	View interface settings on Unix-like systems.
ping	Test reachability and latency.
tracert / traceroute	Map the path to a target.
nslookup / dig	Resolve names and inspect DNS answers.

2. Network and socket checks

netstat -ano	See listening ports and active sessions.
arp -a	Inspect local ARP cache.
route print	Review routing table on Windows.
tcpdump -i eth0	Capture packets on Linux.
Wireshark display filters	Narrow packet views by host, protocol, or field.

3. Security testing basics

nmap -sV	Service/version discovery against a host.
nmap -O	OS detection attempt.
curl -I URL	Fetch HTTP headers quickly.
openssl s_client	Inspect TLS handshakes and certificates.
whois	Gather ownership/registration metadata.

4. Log and process triage

tasklist / ps	List running processes.
taskkill / kill	Terminate a process.
grep / findstr	Search for strings in files or command output.
journalctl	Review Linux journal logs.

Get-EventLog / Get-WinEvent	Query Windows event logs.

5. Exam-useful reminders

Use commands to validate	Do not memorize commands only by name; tie each one to a troubleshooting purpose.
Secure replacements	Know secure replacements like SSH instead of Telnet and SFTP instead of FTP.
Packet first, guess later	Captures and logs beat assumptions.
Evidence handling	In incident questions, document what you collect and preserve integrity.