Security+ SY0-701 Commands Sheet

Core commands and utilities that appear in admin, troubleshooting, and incident-response scenarios.

BEST FOR	FOCUS	USE WITH
Command recognition and what each tool actually does	Windows, Linux, network, packet, and cert basics	Cheat Sheet + Ports Sheet

1. Host and network basics

ipconfig /all - Show Windows IP config, DNS, gateway, MAC, and DHCP details.
ifconfig or ip a - Display Linux interface addresses and status.
ping - Quick reachability check and latency hint; blocked replies do not always mean down.
tracert / traceroute - Show packet path hop by hop.
nslookup / dig - Query DNS records and validate name resolution.

4. Files and integrity

hashfile / certutil -hashfile - Generate a file hash on Windows.
sha256sum - Generate SHA-256 hash on Linux.
chmod - Change Linux file permissions.
chown - Change Linux file ownership.
find - Locate files by name, time, or permission criteria.

2. Active connections and routes

netstat -an - List listening ports and active connections.
ss -tulpn - Linux socket summary with processes and listening services.
route print - Show Windows routing table.
arp -a - View ARP cache to map IP addresses to MAC addresses.
tcpdump -i eth0 - Capture packets on Linux for live troubleshooting.

5. Services and logs

systemctl status - Check Linux service state.
journalctl - Read Linux systemd logs.
Get-EventLog / Get-WinEvent - Review Windows logs in PowerShell.
tasklist - List running processes on Windows.
ps aux - List running processes on Linux.

3. Identity and access

whoami - Display current user and context.
id - Show Linux UID, GID, and group membership.
net user - View or manage local/domain user accounts on Windows.
gpupdate /force - Refresh Group Policy settings.
sudo - Run a command with elevated privileges on Linux.

6. Secure remote access and certs

ssh user@host - Open encrypted remote shell session.
scp file user@host:/path - Copy files securely over SSH.
sftp - Interactive secure file transfer over SSH.
openssl x509 -in cert.pem -text -noout - Inspect certificate details.
nmap -sV target - Enumerate ports and service versions during defensive validation.