SYSTEM PROFILING CHEAT SHEET (Linux)

Main Commands

Command	Description
`ifconfig` *or* `ip`	Network interface configuration
`netstat -tuln`	Open ports and services
`ps`	Process listing
`uname -a`	System information
`lsof -i`	Open file and network information

Commands combinations (You can save all commands in a shell script and run it on the targeted machine, output to a .txt file, and analyze the file later)

Command	Purpose
`ss -tulpen`	Listening sockets + PIDs (modern)
`ip addr; ip route; ip link`	NICs, routes, links
`resolvectl status`	Resolver/DNS
`ps -eo pid,ppid,user,pcpu,pmem,comm --sort=-pcpu | head`	Top CPU processes
`systemctl list-units --type=service --state=running`	Running services
`systemctl list-timers --all; crontab -l`	Timers/cron
`id; who; last -n 10; lastlog | head`	Identity/sessions
`df -h; lsblk -f; mount`	FS and block devices
`du -xh --max-depth=1 / | sort -h | tail`	Big dirs (quick)
`uname -a; lscpu; lspci; lsusb`	Kernel/CPU/devices
`journalctl -p warning -b`	Boot warnings
`journalctl -u svc --since "1 hour ago"`	Service logs
`sudo -l; getenforce/sestatus; aa-status`	Privs + SELinux/AppArmor
`ufw status verbose; firewall-cmd --list-all`	Host firewall status
`nft list ruleset (or iptables -S)`	Packet filter rules
`dpkg -l / rpm -qa`	Installed packages

Helpful Utilities / Containers / Namespaces

Example	Purpose
`...| grep -i PATTERN | tee file.txt`	Search + save
`docker ps -a; docker logs --tail 200 <id>`	Container inventory & logs
`docker inspect <id>`	Container details
`docker exec -it <id> /bin/bash`	Get an interactive shell in a container
`docker stats`	View live container resource usage (CPU, Mem)
`lsns`	List all active system namespaces
`ip netns list`	List network namespaces specifically
`nsenter -t <pid> -n ip addr`	Run command inside a process's network ns

SYSTEM PROFILING CHEAT SHEET (Windows)

Main Commands

Command	Description
`ipconfig /all`	Network configuration details
`netstat -anb`	Active conns, listening ports, executable
`netstat -anob`	As above + PID per connection
`systeminfo`	OS information, patches, hardware
`tasklist /svc`	List of running processes

Windows Essential Commands (PowerShell-first)

Command	Purpose
`whoami /all`	Identity, groups, privileges
`Get-HotFix`	Installed patches/hotfixes
`driverquery /v`	Drivers (verbose)
`Get-NetTCPConnection`	TCP endpoints (modern)
`Resolve-DnsName` *host*	DNS lookups
`Test-NetConnection -ComputerName` *h* `-Port` *n*	TCP reachability
`Get-NetIPConfiguration; Get-NetAdapter`	IP/adapters overview
`Get-Process; Get-Service`	Processes/services
`Get-ScheduledTask`	Scheduled tasks
`Get-WinEvent -LogName System -MaxEvents 50 | fl`	Recent system events
`Get-ComputerInfo`	System inventory (prefer over WMIC)
`sc query; schtasks /query /fo LIST /v`	Legacy svc/tasks

WMIC Commands (*deprecated*)

Command	Info Type
`wmic service list brief`	Service information
`wmic nicconfig get description,IPAddress,MACAddress`	Network configuration
`wmic os get Caption,Version,OSArchitecture,LastBootUpTime`	OS information
`wmic product get name,version`	Installed software
`wmic bios get Manufacturer,Name,Version`	BIOS details
`wmic process list brief`	Process information
`wmic /output:"inventory.html" computersystem list full /format:htable`	Comprehensive output

Helpful Flags (Windows)

Example	Purpose
`ipconfig /all > network_config.txt`	Save output
`netstat -anb | FINDSTR "LISTENING"`	Filter listening ports
`...| findstr /i PATTERN`	Search in output
`...| Select-Object ...| Format-Table -AutoSize`	Tabular view (PS)