Complete Basic Linux + SOC Networking Commands

File and Directory Commands

ls - List directory contents

cd <dir> - Change directory

pwd - Print working directory

mkdir <dir> - Make new directory

rmdir <dir> - Remove empty directory

rm <file> - Remove file

rm -r <dir> - Remove directory recursively

touch <file> - Create empty file

cp <src> <dst> - Copy file

mv <src> <dst> - Move/rename file

find <dir> -name <pattern> - Find files by name

locate <file> - Find file quickly using database

File Content Commands

cat <file> - Display file content

less <file> - Scroll through file

head <file> - First 10 lines

tail <file> - Last 10 lines

tail -f <file> - Live monitor file

wc -l <file> - Count lines

sort <file> - Sort file content

uniq <file> - Remove duplicates

cut -d':' -f1 <file> - Cut specific fields

grep <pattern> <file> - Search for pattern

User Management Commands

whoami - Show current user

id - Show UID, GID

users - Show logged-in users

who - Show logged-in sessions

adduser <user> - Create new user

passwd <user> - Change password

su <user> - Switch user

sudo <command> - Run command as root

groups <user> - Show group membership

Permissions and Ownership

chmod <mode> <file> - Change file permissions

chown <user>:<group> <file> - Change file owner

ls -l - Shows permissions

Software & Package Management (Debian/Ubuntu)

sudo apt update - Update package list

sudo apt upgrade - Upgrade packages

sudo apt install <pkg> - Install package

sudo apt remove <pkg> - Remove package

Process Management

ps aux - List all processes

top - Real-time CPU/memory usage

htop - Interactive version of top

kill <PID> - Terminate a process

kill -9 <PID> - Force kill process

pkill <name> - Kill by name

nice - Set process priority

renice - Change process priority

Disk, System & Hardware Info

df -h - Disk usage

du -sh * - Folder sizes

free -h - RAM usage

uptime - System load info

uname -a - Kernel/system info

hostname - Show or set system name

Archiving & Compression

tar -xvf file.tar - Extract .tar

tar -xzvf file.tar.gz - Extract .tar.gz

zip file.zip file - Compress to .zip

unzip file.zip - Extract .zip

gzip file / gunzip file.gz - Compress/decompress .gz

System & Service Control

systemctl status <service> - Check service status

systemctl start/stop <service> - Control service

systemctl enable/disable <service> - Enable/disable at boot

reboot / shutdown now - Restart or shutdown system

Log Monitoring

journalctl - System logs (systemd)

tail -f /var/log/syslog - Real-time logs

cat /var/log/auth.log - Authentication logs

Basic Linux Networking Commands (SOC)

ip a / ifconfig - Show IP address and interface details

ip r / route -n - Show routing table (gateway info)

ping <IP/hostname> - Test network connectivity

traceroute <IP/hostname> - Show path taken to reach destination

nslookup <domain> - DNS lookup of a domain

nslookup -type=txt <domain> | grep "spf" - SPF DNS lookup

dig <domain> - Detailed DNS query tool

dig +short txt <domain> | grep "spf" - Fetch SPF record

host <domain> - Simple DNS lookup

netstat -antp - Show active TCP connections with process info

ss -tuln - Show listening ports

lsof -i - Show open ports and corresponding processes

tcpdump -i <interface> - Capture and analyze live packets

nmap <IP> - Scan remote system for open ports/services

curl <URL> - Fetch a web page or check HTTP response

wget <URL> - Download a file from the internet

hostname -I - Show system IP address

arp -a - Show ARP table (IP - MAC mapping)

iwconfig - Show Wi-Fi interface settings

nmcli - Manage network connections

Real-Time Network Monitoring

iftop - Show real-time bandwidth usage per connection

nload - Real-time incoming/outgoing traffic graph

vnstat - Network usage statistics over time

Use Cases for Additional SOC Commands

Command	Use Case
$ ip a s	View network interfaces and IPs, useful during asset discovery and compromise validation.
$ find / -iname flag 2>/dev/null	Search system-wide for hidden files or artifacts like 'flag', used in malware hunts.
$ find /usr/share/seclists -name 'name'	Search for specific wordlists (e.g., usernames/passwords) in Seclists repo.
$ id	View UID and GID of current user to assess privilege level.
$ uname -a	Displays OS kernel and architecture info, helpful for identifying exploit potential.
$ whoami	Confirm current user's identity, especially in privilege escalation analysis.
$ cat /etc/*issue	Check for the system version banner, relevant for identifying OS family.
$ cat /etc/*release	Find the Linux distribution and release version essential in vulnerability matching.
$ groups	Lists users group memberships to detect unintended elevated privileges.
$ users	Lists currently logged-in users used in detecting lateral movement or session hijacking.
$ netstat -antp	Identify active TCP connections and corresponding processes, helpful in detecting C2 channels.
$ netstat -tulpn	List all open/listening ports and their associated programs.
$ lsof -i -P	Lists internet sockets with numeric ports good for live investigation.
$ lsof -p <port_number>	Identify which process is bound to a suspicious port.