LSOF – Core Scenarios

Find process using a file:
Command: lsof /var/log/app.log
Use case: Shows PID holding the file. Kill with kill to release it.
List files opened by a user:
Command: lsof -u john
Use case: Audits file usage by a specific user.
Check process using a port:
Command: lsof -i :8080
Use case: Detects port conflicts.
List network connections:
Command: lsof -i
Use case: Shows active network sockets with processes.
Deleted but held file:
Command: lsof | grep deleted
Use case: Finds processes consuming disk via deleted files.
Files open in /tmp:
Command: lsof +D /tmp
Use case: Identifies temp directory abuse.
Process writing to large file:
Command: lsof /path/file
Use case: Detects writers causing file growth.
Sensitive file access:
Command: lsof /etc/passwd
Use case: Security auditing.

Traceroute – Network Diagnosis

Trace path:
Command: traceroute google.com
Use case: Maps packet route and latency.
ICMP mode:
Command: traceroute -I host
Use case: Bypasses UDP blocks.
TCP on HTTPS:
Command: traceroute -T -p 443 host
Use case: Firewall-aware tracing.
Limit hops:
Command: traceroute -m 10 host
Use case: Faster diagnostics.
Increase probes:
Command: traceroute -q 5 host
Use case: Accurate latency checks.

ACL & Permissions Scenario

Create structure:
mkdir -p /data/{finance,hr,it,finance/reports}
Set group ownership:
chown :finance_team /data/finance
chmod 2770 /data/finance
Use case: Ensures group inheritance.
HR read-only:

setfacl -m g:hr_team:rx /data/finance
Exclusive access:
chown bob /data/finance/reports
chmod 700 /data/finance/reports
Default ACLs:
setfacl -d -m g:finance_team:rwx /data/finance

Security & Backup Scenarios

Encrypt backups:
gpg -c file
Use case: Data confidentiality.
Prevent deletion:
chattr +i file
Use case: Protects backups.
Audit access:
auditctl -w /backups/engineering -p rwxa
Use case: Compliance logging.

User & Group Management

Create temp users:
useradd -m -e $(date -d '+30 days' +%F) temp1
Restrict login time:
/etc/security/time.conf
Use case: Time-based access.
Disk quota:
edquota temp1
Use case: Resource control.

Process Management

High CPU:
top / htop
Use case: Identify heavy processes.
Background job:
nohup script.sh &
Use case: Persistent execution.
Change priority:
renice +10 PID
Kill process:
kill PID; kill -9 PID
Resource limit:
ulimit -v 1048576

Network Scenarios

Check port:
ss -lntp | grep 8080
Packet capture:
tcpdump -i eth0 port 22 -w out.pcap

Block IP:
ufw deny from 203.0.113.5
Service check:
systemctl status sshd
Routing:
ip route add 10.1.0.0/24 via GW