MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

PREMIUM PROFESSIONAL REFERENCE · 2026

Linux Security & SysAdmin Command Bible

270 Practical Commands

Three-level command reference for administration, troubleshooting, monitoring, security review, incident response, and hardening.

90	90	90
Basic	Intermediate	Expert

https://mnatech.in/ @mna_tech_academy +91 9216110094

How to use this guide

This reference is designed for legal labs, approved assessments, troubleshooting, and professional learning. Replace placeholders with systems you own or are explicitly authorized to test.

> **Authorization first:** Scanning, exploitation, interception, and administrative commands can disrupt services or expose data. Confirm written scope, use conservative rates, preserve evidence, and stop if impact appears.

Contents

01 · Basic — 90 Commands
Navigation, files, users, processes, networking, services and logs

02 · Intermediate — 90 Commands
Text processing, permissions, packet capture, firewall, SSH, TLS and operations

03 · Expert — 90 Commands
Audit, tracing, isolation, performance, forensics, hardening and cloud-native administration

04 · Tool Selection Matrix
Choose the smallest tool that answers the operational question

05 · Safety & Official References
Operational guardrails and primary manuals

01

Basic — 90 Commands

Navigation, files, users, processes, networking, services and logs

Navigation

Move through and identify filesystem locations

Basic 001 · Navigation

```
pwd
```

Move through and identify filesystem locations

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 002 · Navigation

```
ls -lah
```

Move through and identify filesystem locations

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 003 · Navigation

```
cd /var/log
```

Move through and identify filesystem locations

Note: Review the manual page and test in a non-production environment before applying changes.

Files

Create, copy, move, and inspect files

Basic 004 · Files

```
touch notes.txt
```

Create, copy, move, and inspect files

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 005 · Files

```
cp notes.txt notes.bak
```

Create, copy, move, and inspect files

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 006 · Files

```
mv notes.bak archive.txt
```

Create, copy, move, and inspect files

Note: Review the manual page and test in a non-production environment before applying changes.

Directories

Create and remove empty directory structures

Basic 007 · Directories

```
mkdir -p labs/day1
```

Create and remove empty directory structures

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 008 · Directories

```
rmdir empty-dir
```

Create and remove empty directory structures

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 009 · Directories

```
find . -maxdepth 2 -type d
```

Create and remove empty directory structures

Note: Review the manual page and test in a non-production environment before applying changes.

Text viewing

Read complete or partial text files

Basic 010 · Text viewing

```
cat /etc/os-release
```

Read complete or partial text files

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 011 · Text viewing

```
less /var/log/syslog
```

Read complete or partial text files

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 012 · Text viewing

```
head -n 20 file.txt
```

Read complete or partial text files

Note: Review the manual page and test in a non-production environment before applying changes.

Text tails

Inspect the end of changing logs

Basic 013 · Text tails

```
tail -n 50 /var/log/auth.log
```

Inspect the end of changing logs

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 014 · Text tails

```
tail -f app.log
```

Inspect the end of changing logs

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 015 · Text tails

```
tail -n +10 file.txt
```

Inspect the end of changing logs

Note: Review the manual page and test in a non-production environment before applying changes.

Search text

Find patterns safely

Basic 016 · Search text

```
grep -n "error" app.log
```

Find patterns safely

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 017 · Search text

```
grep -Ri "failed" /var/log
```

Find patterns safely

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 018 · Search text

```
grep -Ev "debug|info" app.log
```

Find patterns safely

Note: Review the manual page and test in a non-production environment before applying changes.

File metadata

Identify file type and metadata

Basic 019 · File metadata

```
file download.bin
```

Identify file type and metadata

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 020 · File metadata

```
stat report.txt
```

Identify file type and metadata

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 021 · File metadata

```
du -h report.txt
```

Identify file type and metadata

Note: Review the manual page and test in a non-production environment before applying changes.

Disk space

Review filesystem capacity and directory usage

Basic 022 · Disk space

```
df -hT
```

Review filesystem capacity and directory usage

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 023 · Disk space

```
du -sh /var/log
```

Review filesystem capacity and directory usage

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 024 · Disk space

```
du -ah . | sort -h
```

Review filesystem capacity and directory usage

Note: Review the manual page and test in a non-production environment before applying changes.

Users

Inspect identity and account records

Basic 025 · Users

```
whoami
```

Inspect identity and account records

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 026 · Users

```
id
```

Inspect identity and account records

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 027 · Users

```
getent passwd
```

Inspect identity and account records

Note: Review the manual page and test in a non-production environment before applying changes.

Sessions

Review logged-in users and activity

Basic 028 · Sessions

```
who
```

Review logged-in users and activity

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 029 · Sessions

```
w
```

Review logged-in users and activity

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 030 · Sessions

```
last -n 20
```

Review logged-in users and activity

Note: Review the manual page and test in a non-production environment before applying changes.

Processes

List and search running processes

Basic 031 · Processes

```
ps aux
```

List and search running processes

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 032 · Processes

```
ps -ef --forest
```

List and search running processes

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 033 · Processes

```
pgrep -af nginx
```

List and search running processes

Note: Review the manual page and test in a non-production environment before applying changes.

Process control

Send controlled signals

Basic 034 · Process control

```
kill -TERM 1234
```

Send controlled signals

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 035 · Process control

```
kill -HUP 1234
```

Send controlled signals

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 036 · Process control

```
pkill -TERM process-name
```

Send controlled signals

Note: Review the manual page and test in a non-production environment before applying changes.

System info

Collect OS and kernel facts

Basic 037 · System info

```
uname -a
```

Collect OS and kernel facts

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 038 · System info

```
hostnamectl
```

Collect OS and kernel facts

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 039 · System info

```
cat /etc/os-release
```

Collect OS and kernel facts

Note: Review the manual page and test in a non-production environment before applying changes.

Network addresses

Review interfaces and routes

Basic 040 · Network addresses

```
ip address show
```

Review interfaces and routes

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 041 · Network addresses

```
ip route show
```

Review interfaces and routes

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 042 · Network addresses

```
ip link show
```

Review interfaces and routes

Note: Review the manual page and test in a non-production environment before applying changes.

Connectivity

Test name resolution and reachability

Basic 043 · Connectivity

```
ping -c 4 192.0.2.1
```

Test name resolution and reachability

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 044 · Connectivity

```
getent hosts example.com
```

Test name resolution and reachability

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 045 · Connectivity

```
resolvectl query example.com
```

Test name resolution and reachability

Note: Review the manual page and test in a non-production environment before applying changes.

Sockets

Review listening and connected sockets

Basic 046 · Sockets

```
ss -tulpn
```

Review listening and connected sockets

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 047 · Sockets

```
ss -tan state established
```

Review listening and connected sockets

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 048 · Sockets

```
ss -s
```

Review listening and connected sockets

Note: Review the manual page and test in a non-production environment before applying changes.

HTTP client

Make controlled web requests

Basic 049 · HTTP client

```
curl -I https://example.com
```

Make controlled web requests

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 050 · HTTP client

```
curl -sS https://example.com/robots.txt
```

Make controlled web requests

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 051 · HTTP client

```
curl -o page.html https://example.com
```

Make controlled web requests

Note: Review the manual page and test in a non-production environment before applying changes.

Download

Retrieve approved files

Basic 052 · Download

```
wget https://example.com/file.txt
```

Retrieve approved files

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 053 · Download

```
wget -c https://example.com/large.iso
```

Retrieve approved files

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 054 · Download

```
curl -LO https://example.com/file.txt
```

Retrieve approved files

Note: Review the manual page and test in a non-production environment before applying changes.

Archives

Create and inspect tar archives

Basic 055 · Archives

```
tar -czf logs.tgz logs/
```

Create and inspect tar archives

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 056 · Archives

```
tar -tzf logs.tgz
```

Create and inspect tar archives

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 057 · Archives

```
tar -xzf logs.tgz
```

Create and inspect tar archives

Note: Review the manual page and test in a non-production environment before applying changes.

Compression

Compress and decompress files

Basic 058 · Compression

```
gzip report.txt
```

Compress and decompress files

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 059 · Compression

```
gunzip report.txt.gz
```

Compress and decompress files

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 060 · Compression

```
xz -z large.log
```

Compress and decompress files

Note: Review the manual page and test in a non-production environment before applying changes.

Permissions

Read and change basic file modes

Basic 061 · Permissions

```
ls -l script.sh
```

Read and change basic file modes

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 062 · Permissions

```
chmod 750 script.sh
```

Read and change basic file modes

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 063 · Permissions

```
chmod u+x script.sh
```

Read and change basic file modes

Note: Review the manual page and test in a non-production environment before applying changes.

Ownership

Review and change file ownership

Basic 064 · Ownership

```
stat -c "%U:%G" file.txt
```

Review and change file ownership

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 065 · Ownership

```
sudo chown alice:analysts file.txt
```

Review and change file ownership

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 066 · Ownership

```
sudo chgrp analysts file.txt
```

Review and change file ownership

Note: Review the manual page and test in a non-production environment before applying changes.

Manuals

Discover syntax and documentation

Basic 067 · Manuals

```
man grep
```

Discover syntax and documentation

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 068 · Manuals

```
grep --help
```

Discover syntax and documentation

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 069 · Manuals

```
apropos "copy files"
```

Discover syntax and documentation

Note: Review the manual page and test in a non-production environment before applying changes.

Environment

Inspect and set shell environment

Basic 070 · Environment

```
printenv
```

Inspect and set shell environment

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 071 · Environment

```
echo "$PATH"
```

Inspect and set shell environment

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 072 · Environment

```
export LAB_MODE=true
```

Inspect and set shell environment

Note: Review the manual page and test in a non-production environment before applying changes.

History

Review shell history responsibly

Basic 073 · History

```
history | tail -n 30
```

Review shell history responsibly

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 074 · History

```
history | grep ssh
```

Review shell history responsibly

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 075 · History

```
fc -l -20
```

Review shell history responsibly

Note: Review the manual page and test in a non-production environment before applying changes.

Date and uptime

Check system time and availability

Basic 076 · Date and uptime

```
date --iso-8601=seconds
```

Check system time and availability

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 077 · Date and uptime

```
timedatectl
```

Check system time and availability

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 078 · Date and uptime

```
uptime
```

Check system time and availability

Note: Review the manual page and test in a non-production environment before applying changes.

Package query

Inspect installed packages

Basic 079 · Package query

```
dpkg -l | head
```

Inspect installed packages

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 080 · Package query

```
apt list --installed
```

Inspect installed packages

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 081 · Package query

```
rpm -qa | head
```

Inspect installed packages

Note: Review the manual page and test in a non-production environment before applying changes.

Services

View service state

Basic 082 · Services

```
systemctl status ssh
```

View service state

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 083 · Services

```
systemctl list-units --type=service
```

View service state

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 084 · Services

```
systemctl is-enabled ssh
```

View service state

Note: Review the manual page and test in a non-production environment before applying changes.

Logs

Read systemd journal

Basic 085 · Logs

```
journalctl -b
```

Read systemd journal

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 086 · Logs

```
journalctl -u ssh --since today
```

Read systemd journal

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 087 · Logs

```
journalctl -p warning
```

Read systemd journal

Note: Review the manual page and test in a non-production environment before applying changes.

Editors

Safely edit configuration text

Basic 088 · Editors

```
nano notes.txt
```

Safely edit configuration text

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 089 · Editors

```
vim notes.txt
```

Safely edit configuration text

Note: Review the manual page and test in a non-production environment before applying changes.

Basic 090 · Editors

```
sed -n "1,40p" config.ini
```

Safely edit configuration text

Note: Review the manual page and test in a non-production environment before applying changes.

02

Intermediate — 90 Commands

Text processing, permissions, packet capture, firewall, SSH, TLS and operations

Find files

Search by name, type, time, and size

Intermediate 001 · Find files

```
find /var/log -type f -name "*.log"
```

Search by name, type, time, and size

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 002 · Find files

```
find . -type f -mtime -1
```

Search by name, type, time, and size

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 003 · Find files

```
find /tmp -type f -size +100M
```

Search by name, type, time, and size

Note: Review the manual page and test in a non-production environment before applying changes.

Locate commands

Resolve executable and database locations

Intermediate 004 · Locate commands

```
command -v python3
```

Resolve executable and database locations

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 005 · Locate commands

```
type -a ssh
```

Resolve executable and database locations

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 006 · Locate commands

```
whereis nginx
```

Resolve executable and database locations

Note: Review the manual page and test in a non-production environment before applying changes.

Advanced grep

Extract context and structured indicators

Intermediate 007 · Advanced grep

```
grep -nC 3 "denied" audit.log
```

Extract context and structured indicators

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 008 · Advanced grep

```
grep -oE "([0-9]{1,3}.){3}[0-9]{1,3}" access.log
```

Extract context and structured indicators

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 009 · Advanced grep

```
grep -RIl "password" ./configs
```

Extract context and structured indicators

Note: Review the manual page and test in a non-production environment before applying changes.

Awk

Select and aggregate columns

Intermediate 010 · Awk

```
awk "{print $1}" access.log
```

Select and aggregate columns

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 011 · Awk

```
awk -F: "{print $1,$7}" /etc/passwd
```

Select and aggregate columns

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 012 · Awk

```
awk "{count[$1]++} END {for (i in count) print i,count[i]}" access.log
```

Select and aggregate columns

Note: Review the manual page and test in a non-production environment before applying changes.

Sed

Print and transform streams

Intermediate 013 · Sed

```
sed -n "20,40p" file.txt
```

Print and transform streams

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 014 · Sed

```
sed "s/secret/[REDACTED]/g" report.txt
```

Print and transform streams

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 015 · Sed

```
sed -E "s/[[:space:]]+/ /g" data.txt
```

Print and transform streams

Note: Review the manual page and test in a non-production environment before applying changes.

Sort and unique

Rank recurring values

Intermediate 016 · Sort and unique

```
sort names.txt
```

Rank recurring values

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 017 · Sort and unique

```
sort ips.txt | uniq -c
```

Rank recurring values

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 018 · Sort and unique

```
sort ips.txt | uniq -c | sort -nr
```

Rank recurring values

Note: Review the manual page and test in a non-production environment before applying changes.

Cut and paste

Extract and combine fields

Intermediate 019 · Cut and paste

```
cut -d: -f1 /etc/passwd
```

Extract and combine fields

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 020 · Cut and paste

```
cut -d" " -f1 access.log
```

Extract and combine fields

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 021 · Cut and paste

```
paste users.txt roles.txt
```

Extract and combine fields

Note: Review the manual page and test in a non-production environment before applying changes.

Xargs

Build controlled argument lists

Intermediate 022 · Xargs

```
find . -name "*.log" -print0 | xargs -0 grep -l error
```

Build controlled argument lists

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 023 · Xargs

```
printf "%s
" a b | xargs -n1 echo
```

Build controlled argument lists

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 024 · Xargs

```
find . -type f -print0 | xargs -0 sha256sum
```

Build controlled argument lists

Note: Review the manual page and test in a non-production environment before applying changes.

Tee

Capture output while displaying it

Intermediate 025 · Tee

```
ip addr | tee network.txt
```

Capture output while displaying it

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 026 · Tee

```
journalctl -u ssh | sudo tee ssh-journal.txt
```

Capture output while displaying it

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 027 · Tee

```
printf "line
" | tee -a notes.txt
```

Capture output while displaying it

Note: Review the manual page and test in a non-production environment before applying changes.

Hashes

Calculate and verify file integrity

Intermediate 028 · Hashes

```
sha256sum image.iso
```

Calculate and verify file integrity

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 029 · Hashes

```
sha256sum -c SHA256SUMS
```

Calculate and verify file integrity

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 030 · Hashes

```
b2sum evidence.bin
```

Calculate and verify file integrity

Note: Review the manual page and test in a non-production environment before applying changes.

ACLs

Inspect and set extended permissions

Intermediate 031 · ACLs

```
getfacl shared.txt
```

Inspect and set extended permissions

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 032 · ACLs

```
setfacl -m u:alice:r shared.txt
```

Inspect and set extended permissions

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 033 · ACLs

```
setfacl -x u:alice shared.txt
```

Inspect and set extended permissions

Note: Review the manual page and test in a non-production environment before applying changes.

Capabilities

Audit Linux file capabilities

Intermediate 034 · Capabilities

```
getcap -r / 2>/dev/null
```

Audit Linux file capabilities

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 035 · Capabilities

```
setcap -v cap_net_bind_service=+ep app
```

Audit Linux file capabilities

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 036 · Capabilities

```
getcap /usr/bin/ping
```

Audit Linux file capabilities

Note: Review the manual page and test in a non-production environment before applying changes.

SUID audit

Find privileged permission bits

Intermediate 037 · SUID audit

```
find / -xdev -perm -4000 -type f 2>/dev/null
```

Find privileged permission bits

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 038 · SUID audit

```
find / -xdev -perm -2000 -type f 2>/dev/null
```

Find privileged permission bits

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 039 · SUID audit

```
stat -c "%A %U:%G %n" /usr/bin/passwd
```

Find privileged permission bits

Note: Review the manual page and test in a non-production environment before applying changes.

Cron

Inspect scheduled tasks

Intermediate 040 · Cron

```
crontab -l
```

Inspect scheduled tasks

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 041 · Cron

```
sudo ls -la /etc/cron.d
```

Inspect scheduled tasks

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 042 · Cron

```
systemctl list-timers --all
```

Inspect scheduled tasks

Note: Review the manual page and test in a non-production environment before applying changes.

System resources

Monitor CPU, memory, and load

Intermediate 043 · System resources

```
top
```

Monitor CPU, memory, and load

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 044 · System resources

```
free -h
```

Monitor CPU, memory, and load

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 045 · System resources

```
vmstat 1 5
```

Monitor CPU, memory, and load

Note: Review the manual page and test in a non-production environment before applying changes.

I/O

Review disk and process I/O

Intermediate 046 · I/O

```
iostat -xz 1 3
```

Review disk and process I/O

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 047 · I/O

```
iotop -o
```

Review disk and process I/O

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 048 · I/O

```
pidstat -d 1 5
```

Review disk and process I/O

Note: Review the manual page and test in a non-production environment before applying changes.

Open files

Map processes to files and sockets

Intermediate 049 · Open files

```
lsof -p 1234
```

Map processes to files and sockets

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 050 · Open files

```
lsof -iTCP -sTCP:LISTEN
```

Map processes to files and sockets

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 051 · Open files

```
lsof +D /var/log
```

Map processes to files and sockets

Note: Review the manual page and test in a non-production environment before applying changes.

Packet capture

Capture narrowly scoped diagnostic traffic

Intermediate 052 · Packet capture

```
sudo tcpdump -i eth0 -nn host 192.0.2.10
```

Capture narrowly scoped diagnostic traffic

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 053 · Packet capture

```
sudo tcpdump -i eth0 -nn port 53
```

Capture narrowly scoped diagnostic traffic

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 054 · Packet capture

```
sudo tcpdump -i eth0 -w capture.pcap -c 500
```

Capture narrowly scoped diagnostic traffic

Note: Review the manual page and test in a non-production environment before applying changes.

Firewall nftables

Inspect modern Linux firewall rules

Intermediate 055 · Firewall nftables

```
sudo nft list ruleset
```

Inspect modern Linux firewall rules

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 056 · Firewall nftables

```
sudo nft list tables
```

Inspect modern Linux firewall rules

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 057 · Firewall nftables

```
sudo nft monitor trace
```

Inspect modern Linux firewall rules

Note: Review the manual page and test in a non-production environment before applying changes.

Firewall iptables

Inspect legacy/netfilter rules

Intermediate 058 · Firewall iptables

```
sudo iptables -L -n -v
```

Inspect legacy/netfilter rules

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 059 · Firewall iptables

```
sudo iptables -S
```

Inspect legacy/netfilter rules

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 060 · Firewall iptables

```
sudo iptables-save
```

Inspect legacy/netfilter rules

Note: Review the manual page and test in a non-production environment before applying changes.

SSH client

Connect and troubleshoot secure shell

Intermediate 061 · SSH client

```
ssh user@192.0.2.10
```

Connect and troubleshoot secure shell

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 062 · SSH client

```
ssh -v user@192.0.2.10
```

Connect and troubleshoot secure shell

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 063 · SSH client

```
ssh -J jump@192.0.2.5 user@192.0.2.10
```

Connect and troubleshoot secure shell

Note: Review the manual page and test in a non-production environment before applying changes.

Secure copy

Transfer approved files securely

Intermediate 064 · Secure copy

```
scp report.txt user@192.0.2.10:/tmp/
```

Transfer approved files securely

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 065 · Secure copy

```
scp user@192.0.2.10:/var/tmp/log.txt .
```

Transfer approved files securely

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 066 · Secure copy

```
rsync -av --progress data/ user@192.0.2.10:/srv/data/
```

Transfer approved files securely

Note: Review the manual page and test in a non-production environment before applying changes.

Certificates

Inspect TLS certificates and handshakes

Intermediate 067 · Certificates

```
openssl x509 -in cert.pem -text -noout
```

Inspect TLS certificates and handshakes

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 068 · Certificates

```
openssl s_client -connect example.com:443 -servername example.com
```

Inspect TLS certificates and handshakes

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 069 · Certificates

```
openssl verify -CAfile ca.pem cert.pem
```

Inspect TLS certificates and handshakes

Note: Review the manual page and test in a non-production environment before applying changes.

DNS tools

Query records and trace delegation

Intermediate 070 · DNS tools

```
dig example.com A
```

Query records and trace delegation

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 071 · DNS tools

```
dig example.com MX +short
```

Query records and trace delegation

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 072 · DNS tools

```
dig +trace example.com
```

Query records and trace delegation

Note: Review the manual page and test in a non-production environment before applying changes.

User administration

Review and manage accounts safely

Intermediate 073 · User administration

```
sudo useradd -m analyst
```

Review and manage accounts safely

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 074 · User administration

```
sudo usermod -aG sudo analyst
```

Review and manage accounts safely

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 075 · User administration

```
sudo passwd -l dormant-user
```

Review and manage accounts safely

Note: Review the manual page and test in a non-production environment before applying changes.

Service changes

Control services with verification

Intermediate 076 · Service changes

```
sudo systemctl restart nginx
```

Control services with verification

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 077 · Service changes

```
sudo systemctl reload nginx
```

Control services with verification

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 078 · Service changes

```
systemctl show nginx --property=ActiveState
```

Control services with verification

Note: Review the manual page and test in a non-production environment before applying changes.

Kernel messages

Inspect boot and driver events

Intermediate 079 · Kernel messages

```
dmesg --level=err,warn
```

Inspect boot and driver events

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 080 · Kernel messages

```
journalctl -k -b
```

Inspect boot and driver events

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 081 · Kernel messages

```
dmesg -T | tail -n 50
```

Inspect boot and driver events

Note: Review the manual page and test in a non-production environment before applying changes.

Mounts

Inspect filesystems and mount options

Intermediate 082 · Mounts

```
findmnt
```

Inspect filesystems and mount options

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 083 · Mounts

```
mount | column -t
```

Inspect filesystems and mount options

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 084 · Mounts

```
findmnt -no TARGET,OPTIONS /tmp
```

Inspect filesystems and mount options

Note: Review the manual page and test in a non-production environment before applying changes.

Containers

Inspect local container state

Intermediate 085 · Containers

```
docker ps --no-trunc
```

Inspect local container state

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 086 · Containers

```
docker inspect container-name
```

Inspect local container state

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 087 · Containers

```
docker logs --since 1h container-name
```

Inspect local container state

Note: Review the manual page and test in a non-production environment before applying changes.

Git audit

Review repository history and change state

Intermediate 088 · Git audit

```
git status --short
```

Review repository history and change state

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 089 · Git audit

```
git log --oneline --decorate -20
```

Review repository history and change state

Note: Review the manual page and test in a non-production environment before applying changes.

Intermediate 090 · Git audit

```
git diff --stat
```

Review repository history and change state

Note: Review the manual page and test in a non-production environment before applying changes.

03

Expert — 90 Commands

Audit, tracing, isolation, performance, forensics, hardening and cloud-native administration

Auditd

Query Linux audit events

Expert 001 · Auditd

```
sudo ausearch -m USER_LOGIN -ts today
```

Query Linux audit events

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 002 · Auditd

```
sudo ausearch -f /etc/passwd
```

Query Linux audit events

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 003 · Auditd

```
sudo aureport --auth
```

Query Linux audit events

Note: Review the manual page and test in a non-production environment before applying changes.

Syscall tracing

Trace a process in a controlled environment

Expert 004 · Syscall tracing

```
strace -f -o trace.log command
```

Trace a process in a controlled environment

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 005 · Syscall tracing

```
strace -e trace=network command
```

Trace a process in a controlled environment

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 006 · Syscall tracing

```
strace -p 1234 -o process.trace
```

Trace a process in a controlled environment

Note: Review the manual page and test in a non-production environment before applying changes.

Library tracing

Observe dynamic library calls

Expert 007 · Library tracing

```
ltrace -o library.trace command
```

Observe dynamic library calls

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 008 · Library tracing

```
ldd /usr/bin/ssh
```

Observe dynamic library calls

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 009 · Library tracing

```
LD_DEBUG=libs command 2>libs.log
```

Observe dynamic library calls

Note: Review the manual page and test in a non-production environment before applying changes.

Namespaces

Inspect process isolation

Expert 010 · Namespaces

```
lsns
```

Inspect process isolation

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 011 · Namespaces

```
nsenter -t 1234 -n ip addr
```

Inspect process isolation

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 012 · Namespaces

```
readlink /proc/1234/ns/net
```

Inspect process isolation

Note: Review the manual page and test in a non-production environment before applying changes.

Cgroups

Review resource-control state

Expert 013 · Cgroups

```
systemd-cgls
```

Review resource-control state

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 014 · Cgroups

```
systemd-cgtop
```

Review resource-control state

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 015 · Cgroups

```
cat /proc/1234/cgroup
```

Review resource-control state

Note: Review the manual page and test in a non-production environment before applying changes.

SELinux

Inspect mandatory access control

Expert 016 · SELinux

```
getenforce
```

Inspect mandatory access control

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 017 · SELinux

```
sestatus
```

Inspect mandatory access control

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 018 · SELinux

```
sudo ausearch -m AVC -ts recent
```

Inspect mandatory access control

Note: Review the manual page and test in a non-production environment before applying changes.

AppArmor

Inspect profile enforcement

Expert 019 · AppArmor

```
sudo aa-status
```

Inspect profile enforcement

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 020 · AppArmor

```
sudo journalctl -k | grep apparmor
```

Inspect profile enforcement

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 021 · AppArmor

```
sudo apparmor_parser -Q /etc/apparmor.d/profile
```

Inspect profile enforcement

Note: Review the manual page and test in a non-production environment before applying changes.

Kernel modules

Inspect loaded kernel code

Expert 022 · Kernel modules

```
lsmod
```

Inspect loaded kernel code

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 023 · Kernel modules

```
modinfo module_name
```

Inspect loaded kernel code

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 024 · Kernel modules

```
cat /proc/modules
```

Inspect loaded kernel code

Note: Review the manual page and test in a non-production environment before applying changes.

Boot analysis

Diagnose boot performance and failures

Expert 025 · Boot analysis

```
systemd-analyze
```

Diagnose boot performance and failures

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 026 · Boot analysis

```
systemd-analyze blame
```

Diagnose boot performance and failures

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 027 · Boot analysis

```
systemd-analyze critical-chain
```

Diagnose boot performance and failures

Note: Review the manual page and test in a non-production environment before applying changes.

Network namespaces

Build isolated network labs

Expert 028 · Network namespaces

```
ip netns list
```

Build isolated network labs

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 029 · Network namespaces

```
sudo ip netns exec lab ip addr
```

Build isolated network labs

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 030 · Network namespaces

```
sudo ip netns exec lab ip route
```

Build isolated network labs

Note: Review the manual page and test in a non-production environment before applying changes.

Advanced routing

Inspect policy routing

Expert 031 · Advanced routing

```
ip rule show
```

Inspect policy routing

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 032 · Advanced routing

```
ip route show table all
```

Inspect policy routing

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 033 · Advanced routing

```
ip route get 192.0.2.10
```

Inspect policy routing

Note: Review the manual page and test in a non-production environment before applying changes.

Neighbor table

Review ARP/NDP state

Expert 034 · Neighbor table

```
ip neigh show
```

Review ARP/NDP state

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 035 · Neighbor table

```
ip neigh show nud failed
```

Review ARP/NDP state

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 036 · Neighbor table

```
ip -6 neigh show
```

Review ARP/NDP state

Note: Review the manual page and test in a non-production environment before applying changes.

Socket internals

Inspect process/socket relationships

Expert 037 · Socket internals

```
ss -plnt
```

Inspect process/socket relationships

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 038 · Socket internals

```
ss -ti dst 192.0.2.10
```

Inspect process/socket relationships

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 039 · Socket internals

```
cat /proc/net/tcp
```

Inspect process/socket relationships

Note: Review the manual page and test in a non-production environment before applying changes.

Traffic control

Inspect shaping and queue disciplines

Expert 040 · Traffic control

```
tc qdisc show
```

Inspect shaping and queue disciplines

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 041 · Traffic control

```
tc class show dev eth0
```

Inspect shaping and queue disciplines

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 042 · Traffic control

```
tc -s filter show dev eth0
```

Inspect shaping and queue disciplines

Note: Review the manual page and test in a non-production environment before applying changes.

eBPF tools

Observe kernel events with installed BCC tools

Expert 043 · eBPF tools

```
sudo execsnoop-bpfcc
```

Observe kernel events with installed BCC tools

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 044 · eBPF tools

```
sudo opensnoop-bpfcc
```

Observe kernel events with installed BCC tools

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 045 · eBPF tools

```
sudo tcpconnect-bpfcc
```

Observe kernel events with installed BCC tools

Note: Review the manual page and test in a non-production environment before applying changes.

Performance perf

Profile CPU behavior

Expert 046 · Performance perf

```
sudo perf top
```

Profile CPU behavior

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 047 · Performance perf

```
sudo perf stat command
```

Profile CPU behavior

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 048 · Performance perf

```
sudo perf record -g command
```

Profile CPU behavior

Note: Review the manual page and test in a non-production environment before applying changes.

Core dumps

Inspect crash configuration and files

Expert 049 · Core dumps

```
coredumpctl list
```

Inspect crash configuration and files

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 050 · Core dumps

```
coredumpctl info 1234
```

Inspect crash configuration and files

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 051 · Core dumps

```
coredumpctl debug 1234
```

Inspect crash configuration and files

Note: Review the manual page and test in a non-production environment before applying changes.

Process memory maps

Inspect mapped regions

Expert 052 · Process memory maps

```
pmap -x 1234
```

Inspect mapped regions

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 053 · Process memory maps

```
cat /proc/1234/maps
```

Inspect mapped regions

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 054 · Process memory maps

```
cat /proc/1234/status
```

Inspect mapped regions

Note: Review the manual page and test in a non-production environment before applying changes.

File attributes

Inspect immutable and append-only flags

Expert 055 · File attributes

```
lsattr file
```

Inspect immutable and append-only flags

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 056 · File attributes

```
sudo chattr +i critical.conf
```

Inspect immutable and append-only flags

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 057 · File attributes

```
sudo chattr -i critical.conf
```

Inspect immutable and append-only flags

Note: Review the manual page and test in a non-production environment before applying changes.

Filesystem forensics

Review deleted-open files and metadata

Expert 058 · Filesystem forensics

```
lsof +L1
```

Review deleted-open files and metadata

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 059 · Filesystem forensics

```
debugfs -R "stat <inode>" image.dd
```

Review deleted-open files and metadata

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 060 · Filesystem forensics

```
fls disk-image.dd
```

Review deleted-open files and metadata

Note: Review the manual page and test in a non-production environment before applying changes.

Disk images

Acquire and validate authorized images

Expert 061 · Disk images

```
sudo dd if=/dev/sdX of=image.dd bs=4M status=progress conv=noerror,sync
```

Acquire and validate authorized images

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 062 · Disk images

```
sha256sum image.dd
```

Acquire and validate authorized images

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 063 · Disk images

```
sudo blockdev --setro /dev/sdX
```

Acquire and validate authorized images

Note: Review the manual page and test in a non-production environment before applying changes.

Journal export

Create structured log exports

Expert 064 · Journal export

```
journalctl -o json > journal.json
```

Create structured log exports

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 065 · Journal export

```
journalctl --since "2026-10-15 00:00" --until "2026-10-15 12:00"
```

Create structured log exports

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 066 · Journal export

```
journalctl --verify
```

Create structured log exports

Note: Review the manual page and test in a non-production environment before applying changes.

System hardening scan

Run locally installed assessment tools

Expert 067 · System hardening scan

```
sudo lynis audit system
```

Run locally installed assessment tools

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 068 · System hardening scan

```
sudo oscap info profile.xml
```

Run locally installed assessment tools

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 069 · System hardening scan

```
sudo systemd-analyze security ssh.service
```

Run locally installed assessment tools

Note: Review the manual page and test in a non-production environment before applying changes.

Package integrity

Verify managed package files

Expert 070 · Package integrity

```
sudo debsums -s
```

Verify managed package files

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 071 · Package integrity

```
rpm -Va
```

Verify managed package files

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 072 · Package integrity

```
dpkg -V package-name
```

Verify managed package files

Note: Review the manual page and test in a non-production environment before applying changes.

SSH server audit

Review effective daemon configuration

Expert 073 · SSH server audit

```
sudo sshd -T
```

Review effective daemon configuration

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 074 · SSH server audit

```
sudo sshd -t
```

Review effective daemon configuration

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 075 · SSH server audit

```
sudo journalctl -u ssh --since today
```

Review effective daemon configuration

Note: Review the manual page and test in a non-production environment before applying changes.

TLS generation

Create lab keys and CSRs

Expert 076 · TLS generation

```
openssl genpkey -algorithm RSA -out lab.key -pkeyopt rsa_keygen_bits:3072
```

Create lab keys and CSRs

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 077 · TLS generation

```
openssl req -new -key lab.key -out lab.csr
```

Create lab keys and CSRs

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 078 · TLS generation

```
openssl pkey -in lab.key -check -noout
```

Create lab keys and CSRs

Note: Review the manual page and test in a non-production environment before applying changes.

JSON processing

Query structured logs and APIs

Expert 079 · JSON processing

```
jq ".[] | .name" data.json
```

Query structured logs and APIs

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 080 · JSON processing

```
jq -r "select(.level=="error") | .message" events.json
```

Query structured logs and APIs

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 081 · JSON processing

```
jq -s "group_by(.source) | map({source:.[0].source,count:length})" events.json
```

Query structured logs and APIs

Note: Review the manual page and test in a non-production environment before applying changes.

YAML processing

Inspect structured configuration with yq

Expert 082 · YAML processing

```
yq ".services" compose.yml
```

Inspect structured configuration with yq

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 083 · YAML processing

```
yq ".spec.template.spec.containers[].image" deployment.yml
```

Inspect structured configuration with yq

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 084 · YAML processing

```
yq -o=json config.yml
```

Inspect structured configuration with yq

Note: Review the manual page and test in a non-production environment before applying changes.

Kubernetes review

Inspect authorized cluster state

Expert 085 · Kubernetes review

```
kubectl auth can-i --list
```

Inspect authorized cluster state

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 086 · Kubernetes review

```
kubectl get pods -A -o wide
```

Inspect authorized cluster state

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 087 · Kubernetes review

```
kubectl get networkpolicy -A
```

Inspect authorized cluster state

Note: Review the manual page and test in a non-production environment before applying changes.

Incident timeline

Build a reproducible event timeline

Expert 088 · Incident timeline

```
find /var/log -type f -printf "%T@ %p
" | sort -n
```

Build a reproducible event timeline

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 089 · Incident timeline

```
journalctl -o short-iso --since today
```

Build a reproducible event timeline

Note: Review the manual page and test in a non-production environment before applying changes.

Expert 090 · Incident timeline

```
last -Faiwx
```

Build a reproducible event timeline

Note: Review the manual page and test in a non-production environment before applying changes.

04

Tool Selection Matrix

Choose the smallest tool that answers the operational question

Question	Start with	Escalate to
Why is a service unavailable?	`systemctl status`, `journalctl -u`, `ss -lntp`	`strace`, packet capture, dependency review
What changed?	`stat`, package history, Git diff	auditd, integrity database, timeline analysis
Who logged in?	`last`, `journalctl`	`ausearch`, identity-provider and network logs
Where is disk space going?	`df`, `du`	`lsof +L1`, filesystem and container layers
Why is the system slow?	`top`, `vmstat`, `iostat`	`pidstat`, `perf`, eBPF tools

05

Safety & Official References

Operational guardrails and primary manuals

Prefer read-only first

Collect state before restarting services, changing permissions, deleting files, or applying firewall rules.

Preserve evidence

Record timestamps, hashes, commands, timezone, host identity, and output location.

Verify destructive targets

Resolve exact paths and devices before `rm`, `dd`, filesystem repair, or recursive ownership changes.

Primary references

`man`, `info`, distribution documentation, kernel.org, systemd.io, OpenSSH manuals.

Keep learning safely

Website
https://mnatech.in/

Instagram
@mna_tech_academy

Call / WhatsApp
+91 9216110094

Practice rule
Only test systems you own or have written authorization to assess.

© 2026 MNA Tech Academy. All rights reserved.
Original educational reference. Product names and trademarks belong to their respective owners. Commands may vary by version and operating system; verify with official documentation before production use.