# Linux CLI: Χρήσιμες εντολές και εργαλεία

CSCGR 2026 - GreekLUG

Στόχος: γρήγορη εικόνα συστήματος, processes/services, ports/dns, αναζήτηση σε αρχεία και βασικός έλεγχος logs. Οι εντολές είναι γενικές και δουλεύουν σε Kali/Ubuntu/Debian (όπου υπάρχει το αντίστοιχο εργαλείο).

## 0) Βοήθεια

| | |
|---|---|
| Γρήγορη βοήθεια: | man <cmd><br><cmd> --help |

## 1) Εικόνα συστήματος

| | |
|---|---|
| Ταυτότητα: | whoami<br>id |
| Πού είμαι:<br>Εμφάνιση αρχείων: | pwd<br>ls -lah |
| Χώρος δίσκου:<br>Χρήση δίσκου: | df -h<br>du -sh ~/* 2>/dev/null \| sort -h \| tail |
| Σύστημα: | uname -a<br>hostnamectl 2>/dev/null \|\| hostname |

## 2) Διεργασίες και υπηρεσίες

| | |
|---|---|
| Top διεργασίες: | ps aux --sort=-%cpu \| head<br>ps aux --sort=-%mem \| head |
| Υπηρεσίες: | systemctl --failed 2>/dev/null \|\| true<br>systemctl status <service> --no-pager 2>/dev/null |

## 3) Δίκτυο και πόρτες

| | |
|---|---|
| Listening ports:<br>Process info:<br>Open files: | ss -tulpen<br>ps -fp <PID><br>lsof |
| Interfaces:<br>Routing: | ip a<br>ip r |
| DNS: | resolvectl status 2>/dev/null \|\| cat /etc/resolv.conf |

## 4) Αρχεία - αναζήτηση και ανάγνωση

| | |
|---|---|
| Ανάγνωση αρχείων: | cat <file> |
| Αναζήτηση αρχείων: | find . -type f -maxdepth 2 \| head |
| Αναζήτηση κειμένου: | grep -Rin "PATTERN" . 2>/dev/null \| head |
| Χειρισμός: | less <file><br>head -n 20 <file><br>tail -n 20 <file> |

## 5) Logs

| | |
|---|---|
| systemd logs: | `journalctl -n 50 --no-pager 2>/dev/null \|\| true`<br>journalctl -u apache2 -n 50 --no-pager 2>/dev/null \|\| true |
| Apache files: | `tail -n 50 /var/log/apache2/access.log 2>/dev/null \|\| true`<br>tail -n 50 /var/log/apache2/error.log 2>/dev/null \|\| true |
| Real-time: | tail -f /var/log/apache2/access.log 2>/dev/null \|\| true |

## 6) Quick patterns σε Apache access.log

```
# Top IPs
awk '{print $1}' access.log | sort | uniq -c | sort -nr | head

# Top requested paths
awk '{print $7}' access.log | sort | uniq -c | sort -nr | head

# Top 404
awk '$9=="404" {print $7}' access.log | sort | uniq -c | sort -nr | head
```

## 7) Έλεγχος αρχείων

```
file suspicious.bin
sha256sum suspicious.bin
strings -n 8 suspicious.bin | head
```

Checklist:

1) εικόνα (whoami/pwd)

2) τι τρέχει (ps/systemctl)

3) τι ακούει (ss)

4) logs (journalctl/tail)

5) αναζήτηση (find/grep)