■ Linux Cheat Sheet (Pentesting Lab)

[Basics]

```
  pwd                # Print working directory
  ls -la             # List files (long + hidden)
  cd /path           # Change directory
  touch file.txt     # Create empty file
  nano file.txt      # Edit file
  cat file.txt       # Show file contents
  cp a.txt b.txt     # Copy file
  mv a.txt dir/      # Move/Rename file
  rm file.txt        # Delete file
```

[User & Permissions]

```
  whoami             # Current user
  id                 # User + groups
  sudo <command>     # Run as root
  chmod 755 file     # Change permissions
  chown user:grp f   # Change owner
```

[Networking]

```
  ifconfig               # Show IPs (use ip a)
  ping 8.8.8.8           # Test connectivity
  traceroute host        # Show packet path
  netstat -tulnp         # List listening ports
  ss -tulnp              # Modern netstat
  dig example.com        # DNS lookup
  nslookup domain        # DNS query
  curl http://site       # Fetch HTTP page
  wget http://site       # Download file
```

[File Searching]

```
  find / -name file.txt        # Search file
  grep "text" file.txt         # Search text
  grep -r "pattern" /dir       # Recursive search
```

[Process Management]

```
  ps aux              # List processes
  top                 # Live process viewer
  kill -9 PID         # Kill process
```

[Package Management]

```
  sudo apt update && sudo apt upgrade -y   # Update system
  sudo apt install nmap -y                 # Install tool
```

[Archives]

```
  tar -cvf files.tar files/    # Create tar
  tar -xvf files.tar           # Extract tar
  gzip file.txt                # Compress
  gunzip file.txt.gz           # Decompress
```

[Cryptography & Hashing]

```
  echo -n "hello" | md5sum     # MD5 hash
  echo -n "hello" | sha256sum  # SHA256 hash
  openssl enc -aes-256-cbc -salt -in file.txt -out file.enc
  openssl enc -d -aes-256-cbc -in file.enc -out file_dec.txt
```

[Nmap]

```
  nmap -sP 192.168.56.0/24   # Ping scan
```

```
nmap -sV target            # Service version
nmap -A target             # Aggressive scan
```

[Wireshark]

```
wireshark                  # Start GUI
Filters: icmp, http, tcp.port==80, ip.addr==192.168.56.101
```

[Netcat]

```
nc -lvp 4444                 # Listener
nc target-ip 4444            # Connect to listener
nc -lvp 4444 > out.txt       # Receive file
nc target-ip 4444 < in.txt   # Send file
```

[Burp Suite]

```
burpsuite                   # Run Burp
Browser proxy -> 127.0.0.1:8080
Intercept HTTP requests
```