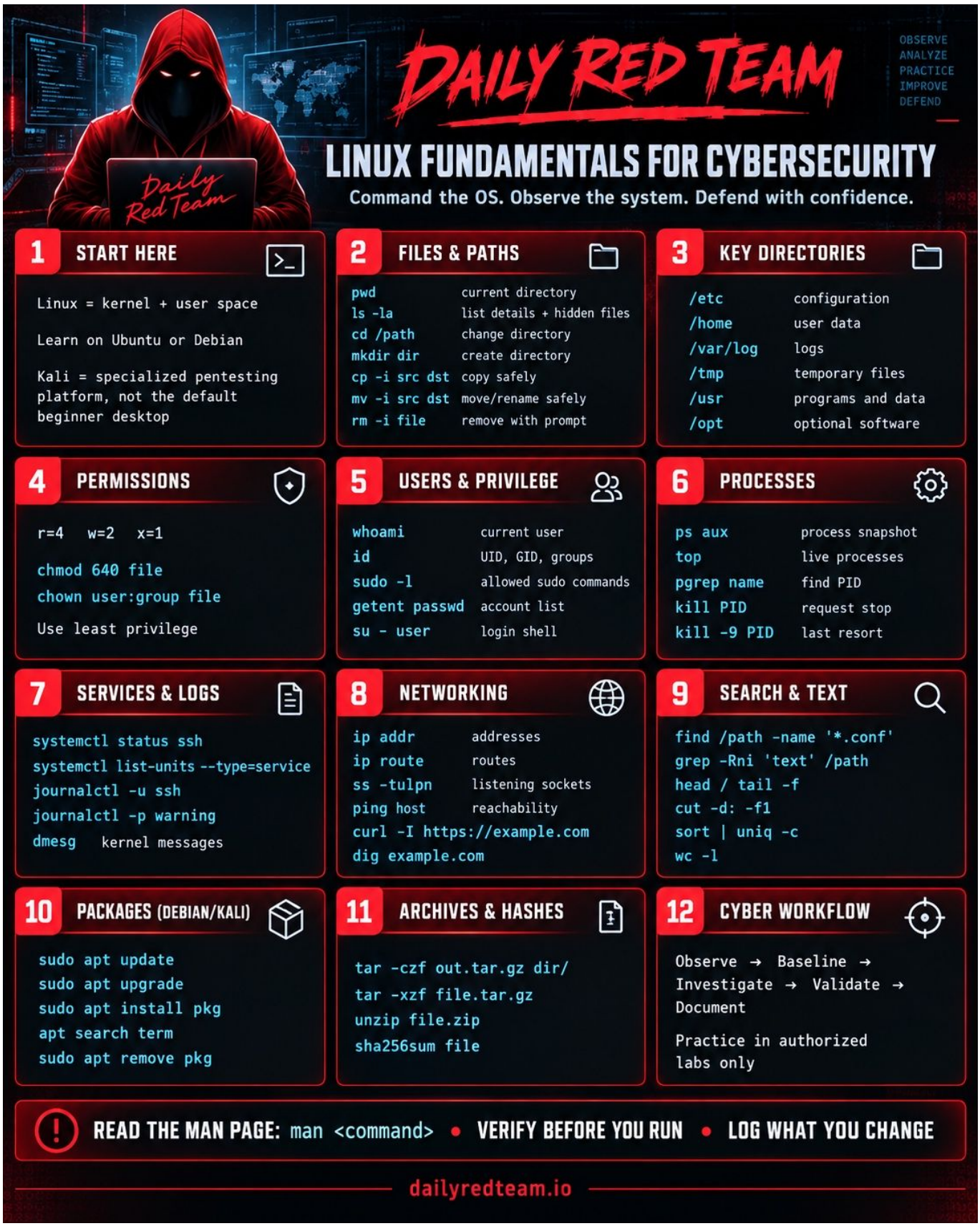
Red Teaming


DAILY RED TEAM
OBSERVE
ANALYZE
PRACTICE
IMPROVE
DEFEND
LINUX FUNDAMENTALS FOR CYBERSECURITY
Command the OS. Observe the system. Defend with confidence.
1 START HERE
Linux = kernel + user space
Learn on Ubuntu or Debian
Kali = specialized pentesting platform, not the default beginner desktop
2 FILES & PATHS
pwd current directory
ls -la list details + hidden files
cd /path change directory
mkdir dir create directory
cp -i src dst copy safely
mv -i src dst move/rename safely
rm -i file remove with prompt
3 KEY DIRECTORIES
/etc configuration
/home user data
/var/log logs
/tmp temporary files
/usr programs and data
/opt optional software
4 PERMISSIONS
r=4 w=2 x=1
chmod 640 file
chown user:group file
Use least privilege
5 USERS & PRIVILEGE
whoami current user
id UID, GID, groups
sudo -l allowed sudo commands
getent passwd account list
su - user login shell
6 PROCESSES
ps aux process snapshot
top live processes
pgrep name find PID
kill PID request stop
kill -9 PID last resort
7 SERVICES & LOGS
systemctl status ssh
systemctl list-units --type=service
journalctl -u ssh
journalctl -p warning
dmesg kernel messages
8 NETWORKING
ip addr addresses
ip route routes
ss -tulpn listening sockets
ping host reachability
curl -I https://example.com
dig example.com
9 SEARCH & TEXT
find /path -name '*.conf'
grep -Rni 'text' /path
head / tail -f
cut -d: -f1
sort | uniq -c
wc -l
10 PACKAGES (DEBIAN/KALI)
sudo apt update
sudo apt upgrade
sudo apt install pkg
apt search term
sudo apt remove pkg
11 ARCHIVES & HASHES
tar -czf out.tar.gz dir/
tar -xzf file.tar.gz
unzip file.zip
sha256sum file
12 CYBER WORKFLOW
Observe → Baseline → Investigate → Validate → Document
Practice in authorized labs only
READ THE MAN PAGE: man <command> • VERIFY BEFORE YOU RUN • LOG WHAT YOU CHANGE
dailyredteam.io