Setup the 'll' command:
    alias ll='clear; ls -lsaht –color=auto'
Check current user:
    whoami;id
Check system info:
    cat /etc/*-release
    uname -a
    printenv
    file /bin/bash
Check available shells:
    cat /etc/shells
Check sudo permissions:
    sudo -l
    subo -V
Check the root directory for anything out of the normal:
    cd /
    ll
Check the /home directory (check each user for ssh keys, bash history, etc):
    cd /home
    ll
Check the /tmp directory:
    cd /tmp
    ll
Check the /dev/shm directory:
    cd /dev/shm
    ll
Check the /opt directory:
    cd /opt
    ll
Check out the /srv directory:
    cd /srv
    ll
Check the /var directory:
    cd /var cd /var/www cd /var/www/html
    ll ll ll
Look for any mail on the system:
    cd /var/mail cd /var/spool/mail
    ll ll
Check the /etc directory:
    cd /etc
    ll
Check /etc/passwd and /etc/shadow:
    ll /etc/passwd – check this to see if its writable
    cat /etc/passwd

    ll /etc/shadow – check this to see if its writable
    cat /etc/shadow
Check CRON:
    ll /etc/cron*

    cd /etc/cron.d
    cat *

cat /etc/crontab

grep -i “CRON” /var/log/syslog

crontab -l

Check the network (we are looking for anything on 127.0.0.1 interface):

netstat -antup

ss -tunlp

Check running services found:

dkpk -l | grep ‘service name’

Check for extended capabilities on any file:

getcap -r / 2>/dev/null

Check SUIDs:

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

Check GUIDs:

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

Check mounts:

mount

cat /etc/fstab

If you don’t find anything in this process, move on to Linpeas

Also try the linux exploit suggestor