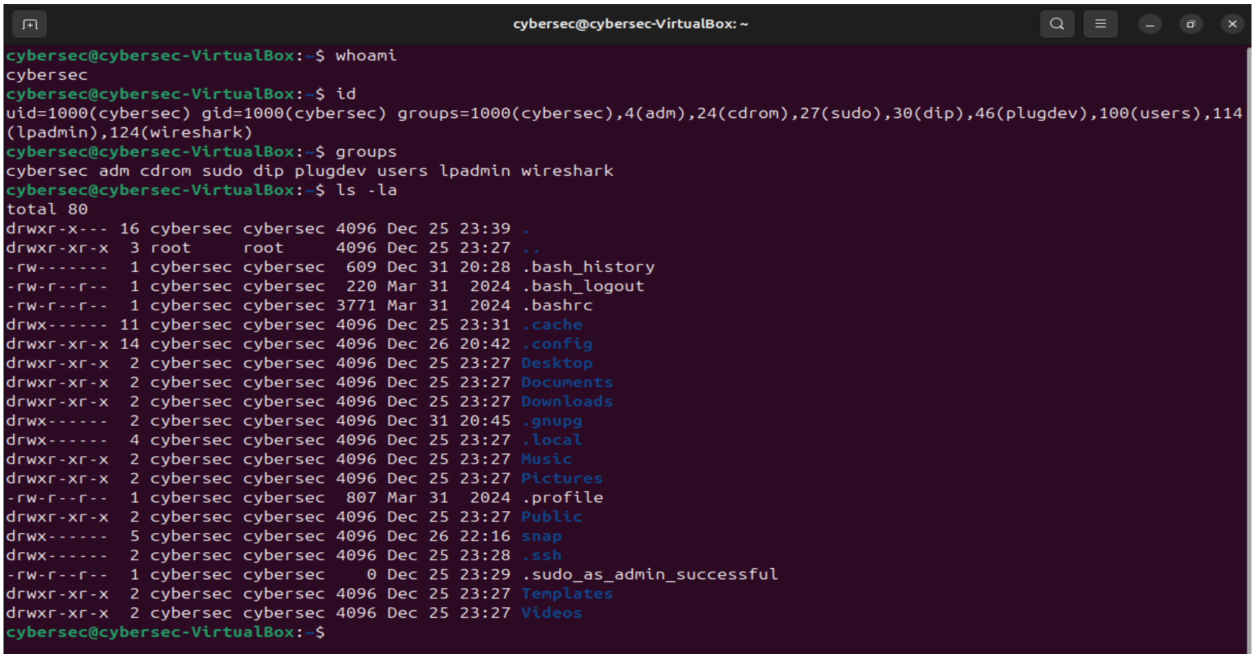
Wireshark week03 notes



```
cybersec@cybersec-VirtualBox:~$ whoami
cybersec
cybersec@cybersec-VirtualBox:~$ id
uid=1000(cybersec) gid=1000(cybersec) groups=1000(cybersec),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users),114
(lpadmin),124(wireshark)
cybersec@cybersec-VirtualBox:~$ groups
cybersec adm cdrom sudo dip plugdev users lpadmin wireshark
cybersec@cybersec-VirtualBox:~$ ls -la
total 80
drwxr-x--- 16 cybersec cybersec 4096 Dec 25 23:39 .
drwxr-xr-x  3 root     root     4096 Dec 25 23:27 ..
-rw-------  1 cybersec cybersec  609 Dec 31 20:28 .bash_history
-rw-r--r--  1 cybersec cybersec  220 Mar 31  2024 .bash_logout
-rw-r--r--  1 cybersec cybersec 3771 Mar 31  2024 .bashrc
drwx------ 11 cybersec cybersec 4096 Dec 25 23:31 .cache
drwxr-xr-x 14 cybersec cybersec 4096 Dec 26 20:42 .config
drwxr-xr-x  2 cybersec cybersec 4096 Dec 25 23:27 Desktop
drwxr-xr-x  2 cybersec cybersec 4096 Dec 25 23:27 Documents
drwxr-xr-x  2 cybersec cybersec 4096 Dec 25 23:27 Downloads
drwx------  2 cybersec cybersec 4096 Dec 31 20:45 .gnupg
drwx------  4 cybersec cybersec 4096 Dec 25 23:27 .local
drwxr-xr-x  2 cybersec cybersec 4096 Dec 25 23:27 Music
drwxr-xr-x  2 cybersec cybersec 4096 Dec 25 23:27 Pictures
-rw-r--r--  1 cybersec cybersec  807 Mar 31  2024 .profile
drwxr-xr-x  2 cybersec cybersec 4096 Dec 25 23:27 Public
drwx------  5 cybersec cybersec 4096 Dec 26 22:16 snap
drwx------  2 cybersec cybersec 4096 Dec 25 23:28 .ssh
-rw-r--r--  1 cybersec cybersec    0 Dec 25 23:29 .sudo_as_admin_successful
drwxr-xr-x  2 cybersec cybersec 4096 Dec 25 23:27 Templates
drwxr-xr-x  2 cybersec cybersec 4096 Dec 25 23:27 Videos
cybersec@cybersec-VirtualBox:~$
```

Desktop directory permissions
drwxr-xr-x

d: directory

OWNER: read, write, execute

GROUP: Read, execute

OTHERS: Read, execute

.ssh directory permissions

drwx------

d: directory

OWNER: read, write, execute

- GROUP: nothing
- OTHERS: nothing

.sudo_as_admin_successful file permissions

-rw-r--r--

- -: file
- OWNER: read, write
- GROUP: read
- OTHERS: read

ps aux - ps aux | grep cybersec - ps aux | head

- a: process for all users
- u: user oriented output (shows, owner, cpu, memory)
- x: processes not tied to a terminal (background/services)

ps aux | head

- User: root
- command: /sbin/init spash
  - First process started by the system

ps aux

- User: cybersec
- command: bash

ps aux | grep daemon | head

- user: root
- command: /usr/sbin/NetworkManager --no-daemon
  - Manages network connections and interfaces.

/var/log – System Logs

The /var/log directory contains system and application logs used for monitoring and security auditing.

auth.log

- Records authentication events such as login attempts, sudo usage, and SSH access
- Security relevance: Used to detect brute-force attacks and unauthorized privilege escalation

syslog

- Contains general system and service messages
- Security relevance: Helps identify abnormal system behavior and correlate security events

kern.log

- Stores kernel-related messages
- Security relevance: Useful for detecting kernel crashes or potential low-level exploits