Below is a table summarizing the user and group management commands you listed (whoami, id, adduser, passwd, su, logout, groups) along with related commands commonly used in Kali Linux. Each row includes the command, its purpose, example usage, and key notes for clarity.

Command	Purpose	Example Usage	Notes
whoami	Displays the username of the current user.	whoami	Outputs current user (e.g., kali). Useful after su or sudo.
id	Shows user ID (UID), group ID (GID), and group memberships.	id or id testuser	Options: -u (UID), -g (GID), -G (all groups).
adduser <name></name>	Interactively creates a new user with home directory and password.	sudo adduser testuser	Preferred over useradd for ease of use; sets up home directory.
passwd <name></name>	Changes the password for a user (or current user if no name given).	passwd or sudo passwd testuser	Requires sudo for other users; critical for security in Kali.
su <user></user>	Switches to another user account (or root if no user specified).	su testuser or su -	su - loads full login environment; sudo -i often preferred in Kali.
logout	Exits the current shell session.	logout	Same as exit; not applicable in GUI sessions.
groups	Lists groups the current user (or specified user) belongs to.	groups or groups testuser	Useful for checking group-based permissions (e.g., wireshark, sudo).
useradd	Low-level command to add a user (less interactive than adduser).	sudo useradd -m -s /bin/bash newuser	Use -m for home directory, -s for shell; requires manual password setup.
usermod	Modifies user account (e.g., add to groups, change shell).	sudo usermod -aG sudo testuser	-aG appends to groups; critical for granting privileges in Kali.
userdel	Deletes a user account.	sudo userdel -r testuser	-r removes home directory; use with caution.
chsh	Changes a user's default shell.	sudo chsh -s /bin/zsh testuser	Common shells in Kali: bash, zsh, fish.

groupadd	Creates a new group.	sudo groupadd pentest	Useful for shared access to pentesting tools.
groupmod	Modifies group settings (e.g., rename group).	sudo groupmod -n security pentest	Rarely used but helpful for group reorganization.
groupdel	Deletes a group.	sudo groupdel pentest	Cannot delete if group is a user's primary group.
gpasswd	Manages group membership or sets group password.	sudo gpasswd -a testuser pentest	Alternative to usermod -aG for adding users to groups.
chmod	Changes file/directory permissions.	chmod 750 script.sh	Relates to your earlier question; e.g., 755 for scripts, 600 for sensitive files.
chown	Changes file/directory owner or group.	sudo chown kali:pentest script.sh	Use -R for recursive changes; critical for securing files in Kali.
chgrp	Changes group ownership of a file/directory.	sudo chgrp pentest script.sh	Similar to chown but only changes group.
sudo	Runs commands as another user (usually root).	sudo apt update	Default kali user has sudo privileges; essential for admin tasks.
sudo -i	Starts an interactive root shell.	sudo -i	Preferred over su - in Kali for root access.
who	Lists all users currently logged in.	who	Shows login sessions; useful for auditing.
w	Shows logged-in users and their activities.	w	Displays user processes and login times.
last	Displays recent login history.	last	Useful for security auditing in Kali.

Notes

- **Kali Linux Context**: These commands are critical for managing users and permissions in Kali, especially for securing pentesting tools and environments.
- **Security**: Use sudo carefully, set strong passwords with passwd, and restrict permissions with chmod/chown to protect sensitive files.

- **File Access**: Check /etc/passwd, /etc/shadow (requires sudo), and /etc/group for user and group details.
- **Best Practice**: Regularly audit users (who, last) and groups (groups, id) to ensure no unauthorized access.

If you need a specific example (e.g., setting up a user with permissions for a pentesting tool) or a visual chart (e.g., user-group relationships), let me know!

Best Practices in Kali Linux

- **Use sudo**: Kali's default user (kali) has sudo privileges, so prefer sudo over su for administrative tasks.
- **Secure Passwords**: Use passwd to set strong passwords, especially for root or pentesting users.
- **Minimal Privileges**: Add users to groups (e.g., wireshark, sudo) only when necessary to limit access.
- **Audit Users/Groups**: Regularly check id, groups, or /etc/group to ensure no unauthorized users have elevated privileges.
- **Lock Down Files**: Use chmod and chown to restrict access to sensitive pentesting scripts or logs (e.g., chmod 600 report.txt).
- **Monitor Logins**: Use who, w, or last to monitor active users, especially on shared Kali systems.

---

topic 1: Introduction to Kali Linux and Terminal Basics

- **Objective**: Understand Kali Linux and basic navigation commands.
- **Lab Activities** :
    - Log into Kali Linux (default user: `kali`).
    - Run `pwd` to find current directory.
    - Use `ls`, `ls -l`, `ls -a` to explore `/home/kali`.
    - Navigate with `cd /etc`, `cd ..`, `cd ~`.
- **Deliverable**: Screenshot of `ls -l` output in `/etc`.
- **Notes**: Discuss Kali's pentesting focus; explain `ls -l` permission format (e.g., `rwxr-xr-x`).

Command	Description	Example
`pwd`	Print current directory path	`pwd`
`ls`	List directory contents	`ls`
`ls -l`	Long listing format (shows permissions)	`ls -l /etc`
`ls -a`	Show hidden files	`ls -a`
`cd <dir>`	Change directory	`cd /etc`
`cd ..`	Go up one directory	`cd ..`

- **Practice Problems** (30 min):
    1. Navigate to `/var/log`, list all files (including hidden) with details, and submit the output of `ls -la`.
    2. Use `pwd` and `cd` to move from `/home/kali` to `/usr/share`, then back to `/home/kali`. Submit a screenshot of the final `pwd` output.

---

topic 2: File and Directory Management

- **Objective**: Create and delete files/directories.
- **Lab Activities** :
    - Create a directory: `mkdir pentest-lab`.
    - Create a file: `touch report.txt`.
    - Remove file: `rm report.txt`.
    - Create and remove a directory: `mkdir temp`, `rmdir temp`.
    - Delete non-empty directory: `rm -r pentest-lab`.
- **Deliverable**: Screenshot of `ls -l pentest-lab/`.
- **Notes**: Highlight risks of `rm -r`; connect to permissions (`rwxr`).

Command	Description	Example
`mkdir <dir>`	Create a new directory	`mkdir pentest-lab`
`rmdir <dir>`	Remove empty directory	`rmdir temp`
`rm -r <dir>`	Remove directory and contents	`rm -r pentest-lab`
`rm <file>`	Delete file	`rm report.txt`
`touch <file>`	Create empty file	`touch report.txt`

- **Practice Problems** (30 min):
    1. Create a directory `lab2` with a subdirectory `scripts` and a file `test.txt` inside it. Submit `ls -l lab2/scripts/`.
    2. Create a directory `temp_dir`, add two files (`file1.txt`, `file2.txt`), then delete `temp_dir` recursively. Submit a screenshot confirming deletion (`ls -l` shows no `temp_dir`).

---

topic 3: File Copying and Moving

- **Objective**: Copy and move files/directories.
- **Lab Activities** :
    - Create: `touch script.sh`.
    - Copy: `cp script.sh script_backup.sh`.
    - Move: `mv script_backup.sh pentest-lab/`.
    - Verify: `ls -l pentest-lab/`.
- **Deliverable**: Screenshot of `ls -l pentest-lab/` showing copied/moved files.
- **Notes**: Discuss `cp -r` for directories.

Command	Description	Example
`cp file1 file2`	Copy file	`cp script.sh script_backup.sh`
`mv file1 file2`	Move or rename file	`mv script_backup.sh pentest-lab/`

- **Practice Problems** (30 min):
    1. Create a file `notes.txt`, copy it to `notes_backup.txt` in `pentest-lab/`, and submit `ls -l pentest-lab/`.
    2. Rename `notes.txt` to `notes_old.txt` using `mv` and submit `ls -l` showing the renamed file.

---

topic 4: Viewing File Contents

- **Objective**: Display file contents.
- **Lab Activities** :
    - Create: `cat > test.txt` (type text, Ctrl+D).
    - View: `cat test.txt`, `more test.txt`, `less test.txt`.
    - Check lines: `head test.txt`, `tail test.txt`.
    - Concatenate: `cat test.txt test2.txt`.
- **Deliverable**: Screenshot of `cat test.txt test2.txt`.
- **Notes**: Explain `less` for large files; relate to `/etc/group`.

Command	Description	Example
`cat <file>`	Display file contents	`cat test.txt`
`cat file1 file2`	Display multiple files	`cat test.txt test2.txt`
`more <file>`	View file one screen at a time	`more test.txt`
`less <file>`	View file with navigation	`less test.txt`
`head <file>`	View beginning of file	`head test.txt`
`tail <file>`	View end of file	`tail test.txt`

- **Practice Problems** (30 min):
    1. Create two files (`log1.txt`, `log2.txt`) with sample text, concatenate them using `cat`, and submit the output.
    2. Use `less` to view `/etc/passwd` and `head` to show its first 5 lines. Submit screenshots of both.

---

topic 5: File Creation and Appending

- **Objective**: Create and append to files using `cat`.
- **Lab Activities** :
  - Create: `cat > report.txt` (type text, Ctrl+D).
  - Append: `cat >> report.txt`.
  - Copy: `cat report.txt > report_copy.txt`.
  - Append: `cat report.txt >> report_copy.txt`.
- **Deliverable**: Screenshot of `cat report_copy.txt`.
- **Notes**: Discuss overwrite vs. append.

Command	Description	Example
`cat > file`	Create file with keyboard input	`cat > report.txt`
`cat >> file`	Append text to file	`cat >> report.txt`
`cat file1 > file2`	Copy contents (overwrite)	`cat report.txt > report_copy.txt`
`cat file1 >> file2`	Append contents	`cat report.txt >> report_copy.txt`

- **Practice Problems** (30 min):
  1. Create `data.txt` with `cat`, append a second line, and submit `cat data.txt`.
  2. Copy `data.txt` to `data_backup.txt` and append `data.txt` to it again. Submit `cat data_backup.txt`.

---

topic 6: File Editing with Nano

- **Objective**: Edit files using Nano.
- **Lab Activities** :
    - Open: `nano script.sh`.
    - Add text (e.g., `#!/bin/bash`), save (`Ctrl+O`, Enter), exit (`Ctrl+X`).
    - Search: `Ctrl+W`, type “bash”, find next (`Alt+W`).
    - Replace: `Ctrl+\`, enter terms.
- **Deliverable**: Screenshot of `cat script.sh`.
- **Notes**: Install Nano: `sudo apt install nano`.

Command/Shortcut	Description	Example
`nano <file>`	Open file in Nano	`nano script.sh`
`Ctrl + O, Enter`	Save changes	`Ctrl + O`
`Ctrl + X`	Exit Nano	`Ctrl + X`
`Ctrl + W`	Search for text	`Ctrl + W`, type “bash”
`Ctrl + \`	Replace text	`Ctrl + \`, enter terms

- **Practice Problems** (30 min):
    1. Create `notes.txt` in Nano, add 3 lines about Kali Linux, and submit `cat notes.txt`.
    2. In `notes.txt`, search for “Kali” and replace with “Linux”. Submit the updated `cat notes.txt`.

---

topic 7: File Editing with Vim

- **Objective**: Learn basic Vim editing.
- **Lab Activities** :
    - Open: `vim notes.txt`.
    - Insert mode (`i`), add text, save (`:w`), exit (`:q`).
    - Save and exit: `:wq`.
- **Deliverable**: Screenshot of `cat notes.txt`.
- **Notes**: Explain Vim modes.

Command/Shortcut	Description	Example
`vim <file>`	Open file in Vim	`vim notes.txt`
`i`	Enter insert mode	`i`
`:w`	Save changes	`:w`
`:q`	Exit Vim	`:q`
`:wq`	Save and exit	`:wq`

- **Practice Problems** (30 min):
    1. Create `vim_test.txt` in Vim, add 2 lines, and submit `cat vim_test.txt`.
    2. Edit `vim_test.txt` to add a third line and submit the updated file.

---

topic 8: Writing to Files with Echo

- **Objective**: Write/append text using `echo`.
- **Lab Activities** :
  - Write: `echo "Pentest report" > report.txt`.
  - Append: `echo "Aug 2025" >> report.txt`.
  - Verify: `cat report.txt`.
- **Deliverable**: Screenshot of `cat report.txt`.
- **Notes**: Compare with `cat > file`.

Command	Description	Example
`echo "text" > file.txt`	Write text to file (overwrite)	`echo "Pentest report" > report.txt`
`echo "text" >> file.txt`	Append text to file	`echo "Aug 2025" >> report.txt`

- **Practice Problems** (30 min):
  1. Use `echo` to create `log.txt` with “System check” and submit `cat log.txt`.
  2. Append “Completed: 2025” to `log.txt` and submit the updated file.

---

topic 9: User Management Basics

- **Objective**: Create and manage users.
- **Lab Activities** :
  - Check: `whoami`, `id`.
  - Create: `sudo adduser pentester`.
  - Set password: `sudo passwd pentester`.
- **Deliverable**: Screenshot of `id pentester`.
- **Notes**: Link to `sudoers` fix.

Command	Description	Example
`whoami`	Show current user	`whoami`
`id`	Show user ID and groups	`id pentester`
`sudo adduser <name>`	Create new user	`sudo adduser pentester`
`su <user>`	Switch user	`su pentester`

- **Practice Problems** (30 min):
  1. Create a user `tester` and submit `id tester`.
  2. Change `tester`'s password and verify login with `su tester` (submit `whoami` output).

---

topic 10: Switching Users and Logging Out

- **Objective**: Switch users and manage sessions.
- **Lab Activities** :
  - Switch: `su pentester`.
  - Verify: `whoami`, `id`.
  - Log out: `logout` or `exit`.
- **Deliverable**: Screenshot of `whoami` as `pentester`.
- **Notes**: Compare `su` vs. `sudo -i`.

Command	Description	Example
`passwd <name>`	Change user password	`sudo passwd pentester`
`logout`	Log out of shell session	`logout`
`exit`	Log out (alternative)	`exit`

- **Practice Problems** (30 min):
  1. Switch to `pentester`, run `whoami`, and submit the output.
  2. Switch to `pentester`, run `id`, log out, and submit `id` output as `kali`.

topic 11: Group Management

- **Objective**: Create and manage groups.
- **Lab Activities** :
    - Create: `sudo groupadd pentest`.
    - Add user: `sudo usermod -aG pentest pentester`.
    - Verify: `groups pentester`, `cat /etc/group | grep pentest`.
- **Deliverable**: Screenshot of `cat /etc/group | grep pentest`.
- **Notes**: Link to `rwxr-x---`.

Command	Description	Example
`groupadd`	Create new group	`sudo groupadd pentest`
`groups`	Show user's group membership	`groups pentester`
`cat /etc/group	grep pentest`	Check group details	
`usermod -aG <group> <user>`	Add user to a group	`sudo usermod -aG pentest pentester`

- **Practice Problems** (30 min):
    1. Create a group `security`, add `pentester` to it, and submit `grep security /etc/group`.
    2. Verify `pentester`'s groups with `groups pentester` and submit the output.

---

topic 12: File Permissions

- **Objective**: Set and understand file permissions.
- **Lab Activities** :
    - Check: `ls -l script.sh`.
    - Set: `chmod 755 script.sh` (`rwxr-xr-x`).
    - Make executable: `chmod +x script.sh`.
- **Deliverable**: Screenshot of `ls -l script.sh` showing `rwxr-xr-x`.
- **Notes**: Explain `r=4`, `w=2`, `x=1`.

Command	Description	Example
`ls -l`	Show file permissions	`ls -l script.sh`
`chmod 755 <file>`	Set permissions (rwxr-xr-x)	`chmod 755 script.sh`
`chmod +x <file>`	Make file executable	`chmod +x script.sh`

- **Practice Problems** (30 min):
    1. Create `test.sh`, set permissions to `rwxr-x---` (750), and submit `ls -l test.sh`.
    2. Make `test.sh` executable with `chmod +x` and submit `ls -l` output.

---

topic 13: File Ownership and Sudo

- **Objective**: Manage file ownership and fix `sudoers` issues.
- **Lab Activities** :
    - Change ownership: `sudo chown pentester:pentest script.sh`.
    - Fix `sudoers`: `sudo usermod -aG sudo pentester`.
    - Verify: `ls -l script.sh`, `groups pentester`.
- **Deliverable**: Screenshot of `ls -l` showing ownership.
- **Notes**: Relate to `pentest` group.

Command	Description	Example
`chown user:group <file>`	Change owner and group	`sudo chown pentester:pentest script.sh`
`sudo`	Run as root user	`sudo ls`
`usermod -aG sudo <user>`	Add user to sudo group	`sudo usermod -aG sudo pentester`

- **Practice Problems** (30 min):
    1. Change ownership of `test.sh` to `pentester:pentest` and submit `ls -l test.sh`.
    2. Add `tester` to `sudo` group and verify with `groups tester`.

---

topic 14: Software Installation with APT

- **Objective**: Install and manage packages.
- **Lab Activities** :
    - Update: `sudo apt update`.
    - Install: `sudo apt install htop`.
    - List: `apt list --installed | grep htop`.
- **Deliverable**: Screenshot of `apt list --installed | grep htop`.
- **Notes**: Emphasize Kali's tools.

Command	Description	Example
`sudo apt update`	Update package list	`sudo apt update`
`sudo apt upgrade`	Upgrade installed packages	`sudo apt upgrade`
`sudo apt install <package>`	Install a package	`sudo apt install htop`
`apt list --installed`	List installed packages	`apt list --installed`

- **Practice Problems** (30 min):
    1. Install `tree` package and submit `apt list --installed | grep tree`.
    2. Update package list and upgrade, submitting `sudo apt upgrade` output.

---

topic 15: System Monitoring

- **Objective**: Monitor system resources.
- **Lab Activities** :
    - Monitor: `top`, `htop`.
    - Check processes: `ps aux | grep bash`.
    - View resources: `free -h`, `df -h`, `du -sh /pentest-lab`.
- **Deliverable**: Screenshot of `htop` output.
- **Notes**: Link to pentesting resource needs.

Command	Description	Example
`top`	Live system monitoring	`top`
`htop`	Enhanced top	`htop`
`ps aux`	View running processes	`ps aux`
`free -h`	Check memory usage	`free -h`
`df -h`	Show disk space	`df -h`
`du -sh <dir>`	Size of a directory	`du -sh /pentest-lab`

- **Practice Problems** (30 min):
    1. Run `top`, identify a process PID, and submit a screenshot.
    2. Check disk usage of `/home` with `du -sh /home` and submit the output.

---

topic 16: Networking Basics

- **Objective**: Explore network configuration.
- **Lab Activities** :
    - Check: `ip a`.
    - Test: `ping 8.8.8.8`.
    - View ports: `netstat -tuln`.
    - Fetch: `curl example.com`.
- **Deliverable**: Screenshot of `ip a` output.
- **Notes**: Relate to Kali's networking tools.

Command	Description	Example
`ip a`	Show IP configuration	`ip a`
`ping <host>`	Test connectivity	`ping 8.8.8.8`
`netstat -tuln`	Show listening ports	`netstat -tuln`
`curl <url>`	Fetch a webpage	`curl example.com`

- **Practice Problems** (30 min):
    1. Ping `google.com` and submit the first 4 lines of output.
    2. Run `netstat -tuln` and submit a screenshot of active ports.

---

topic 17: Advanced Networking

- **Objective**: Use advanced networking tools.
- **Lab Activities** :
    - Trace: `traceroute google.com`.
    - DNS: `nslookup google.com`, `dig google.com`.
    - Download: `wget example.com/index.html`.
- **Deliverable**: Screenshot of `dig google.com`.
- **Notes**: Emphasize pentesting applications.

Command	Description	Example
`traceroute <host>`	Show route to host	`traceroute google.com`
`nslookup <domain>`	DNS lookup	`nslookup google.com`
`dig <domain>`	Advanced DNS lookup	`dig google.com`
`wget <url>`	Download file from URL	`wget example.com/index.html`

- **Practice Problems** (30 min):
    1. Run `dig example.com` and submit the output.
    2. Download a file with `wget` from a public URL and submit `ls -l` showing the file.

---

topic 18: Service Management

- **Objective**: Manage system services.
- **Lab Activities** :
    - Check: `systemctl status ssh`.
    - Start/stop: `sudo systemctl start ssh`, `sudo systemctl stop ssh`.
    - View logs: `journalctl -u ssh`.
- **Deliverable**: Screenshot of `systemctl status ssh`.
- **Notes**: Discuss `ssh` in Kali.

Command	Description	Example
`systemctl status <service>`	Check service status	`systemctl status ssh`
`systemctl start <service>`	Start a service	`sudo systemctl start ssh`
`systemctl stop <service>`	Stop a service	`sudo systemctl stop ssh`
`systemctl restart <service>`	Restart service	`sudo systemctl restart ssh`
`journalctl`	View system logs	`journalctl -u ssh`

- **Practice Problems** (30 min):
    1. Start the `ssh` service and submit `systemctl status ssh`.
    2. View recent `ssh` logs with `journalctl -u ssh | tail` and submit the output.

---

topic 19: Bash Scripting Basics

- **Objective**: Write and run Bash scripts.
- **Lab Activities** :

Create: `nano script.sh`, add:
#!/bin/bash
echo "Hello, Kali!"

    -
    - Make executable: `chmod +x script.sh`.
    - Run: `./script.sh`.
- **Deliverable**: Screenshot of `./script.sh` output.
- **Notes**: Link to `chmod +x`.

Command	Description	Example
`#!/bin/bash`	Shebang (top of script)	`#!/bin/bash` in script.sh
`echo "text"`	Print text	`echo "Hello, Kali!"`
`chmod +x script.sh`	Make script executable	`chmod +x script.sh`
`./script.sh`	Run script	`./script.sh`

- **Practice Problems** (30 min):
    1. Create a script `hello.sh` that prints “Welcome to Kali” and submit its output.
    2. Modify `hello.sh` to print the current directory (`pwd`) and submit the output.

---

topic 20: Search, Filters, and Cleanup

- **Objective**: Search files and maintain the system.
- **Lab Activities** :
    - Search: `grep pentest /etc/group`.
    - Find: `find /home -name report.txt`.
    - Clean: `sudo apt autoremove`.
    - History: `history | tail`.
- **Deliverable**: Screenshot of `grep pentest /etc/group`.
- **Notes**: Reinforce `grep` from earlier.

Command	Description	Example
`grep "text" file.txt`	Find text in file	`grep pentest /etc/group`
`find / -name file.txt`	Locate file	`find /home -name report.txt`
`sudo apt autoremove`	Remove unused packages	`sudo apt autoremove`
`history`	Show recent commands	`history

- **Practice Problems** (30 min):
    1. Search for “kali” in `/etc/passwd` with `grep` and submit the output.
    2. Find all `.txt` files in `/home` with `find` and submit the results.

General Notes

- **Environment**: Use Kali Linux VMs (e.g., VirtualBox).
- **Permissions**: Use `chmod 750` (`rwxr-x---`) for secure group access (e.g., `pentest`).
- **Security**: Add users to `sudo` group (`usermod -aG sudo pentester`) only for trusted users.
- **Resources**:
    - Kali Docs: https://www.kali.org/docs/
    - Linuxize: https://linuxize.com/post/how-to-create-users-in-linux/
- **Assessment**: Weekly deliverables (screenshots, scripts) and a final project: Create a user (`pentester`), group (`pentest`), script, and secure it with `chmod 750`.