Got it — you’re now in **post-exploitation** territory and looking at **Privilege Escalation** after getting a foothold.  
Here’s the short structured breakdown for you:

**Privilege Escalation in Pentesting**

Once you gain access to a target system (low-privileged user), the goal is to elevate privileges to **admin/root** to gain full control.

**1. Types of Privilege Escalation**

* **Horizontal** – Gain access to other user accounts with similar privileges.
* **Vertical** – Increase privileges to admin/root level.

**2. Common Windows Privilege Escalation Techniques**

* **Check Sudo/Sudoers Misconfigurations** (Linux equivalent is sudo -l in Linux, here check if user is in Administrators group).
* **Unpatched Vulnerabilities** – Kernel exploits (e.g., MS16-032, PrintNightmare).
* **Misconfigured Services** – Weak permissions on service executables or DLL hijacking.
* **Stored Credentials** – Search memory, config files, registry for saved passwords (mimikatz).
* **AlwaysInstallElevated** – If enabled, allows running MSI packages with SYSTEM privileges.

**3. Common Linux Privilege Escalation Techniques**

* **SUID/SGID Files** – Files with SUID bit set that can be abused (find / -perm -4000 2>/dev/null).
* **GTFOBins** – Lookup binaries that can be exploited to get a shell.
* **Kernel Exploits** – Check kernel version for local privilege escalation exploits.
* **Writable /etc/passwd or /etc/sudoers** – Misconfigurations allowing privilege gain.
* **Cron Jobs** – Writable scripts executed by root.

**4. Tools & Scripts for Enumeration**

* **Windows:** winPEAS, PowerUp.ps1, Seatbelt.exe
* **Linux:** linPEAS, Linux Exploit Suggester, pspy
* **Manual Enumeration:** whoami, id, uname -a, hostname, netstat -tulnp

**5. General Workflow**

1. **Enumerate** system info, network, services, and users.
2. **Search for Misconfigurations** (SUID, sudoers, writable files).
3. **Check for Exploitable Vulnerabilities** based on OS and version.
4. **Exploit** and escalate to root/admin.
5. **Maintain Access** (backdoor, persistence).

If you want, I can give you a **step-by-step privilege escalation checklist** you can follow *every time* you pop a shell — so you won’t miss anything during an engagement.  
That way, you’ll always know exactly what to do next after Metasploit access.