**Initial Server Setup (Windows Server 2025 Standard)**

**What is This About?**

This phase is all about preparing the foundation of an enterprise-grade server environment using **Windows Server 2025 Standard**. A proper initial setup ensures the machine is secure, manageable, and ready to handle roles like Active Directory, DNS, and File Services.

**Why is This Important in Real-World Environments?**

* Prevents misconfigurations that lead to **vulnerabilities**
* Sets the stage for **Active Directory**, DNS, DHCP, File Servers
* Establishes **network identity** and **admin controls**
* A solid initial setup prevents lateral movement, unauthorized access, and instability

**How It Helps Protect an organization**

| **Misstep** | **Risk** | **Secure Setup Fix** |
| --- | --- | --- |
| Default admin name | Targeted attacks like brute force | Rename and disable defaults |
| No firewall hardening | Open ports to attackers | Controlled rule sets |
| Weak passwords | Easy privilege escalation | Group password policies |
| Dynamic IP for server | DNS failures / spoofing | Static IP for consistency |

**My Home Lab Setup:**

| **Item** | **Value** |
| --- | --- |
| **Server OS** | Windows Server 2025 Standard |
| **Host Machine** | Personal Laptop |
| **Virtualization** | Hyper-V |
| **Static IP** | 192.168. XX. XX |
| **Server Name** | PRK-SRV01 |
| **Domain** | xyz.local |

**Step-by-Step: What I Did**

**1.Renamed Server and Set Hostname:**

****

* Renaming the server helps with organization, clarity in logs, and future Active Directory integration.

**2. Create a Custom Admin Account**

**For Ex:**

****

**What it does:**

* **net user:** Classic Windows command-line utility to manage user accounts.
* **praki-admin:** The username to create.
* **StrongPassword123!:** Sets the account password (choose a strong one).
* **/add:** Adds the new account to the system.
* **net localgroup:** Manages local user groups.
* **administrators:** The name of the group.
* **praki-admin:** The user to add.
* **/add:** Adds the user to the specified group.

**Why it's useful:**

* You should never use the default **"Administrator"** account in production.
* Creating a custom admin account helps obscure attack targets and enhances auditing.
* Gives your new user **full administrative rights** on the machine.
* Still allows tracking specific actions via praki-admin instead of default admin.

**Then disable the built-in Administrator account:**

****

**What it does:**

* net user Administrator: Targets the built-in Administrator account.
* /active:no: Disables the account from logging in.

**Why it's useful:**

* Disabling the built-in admin account is standard hardening to reduce brute-force and known-user attacks.

**3. Enable Remote Desktop & Firewall Rule**

****

**What it does:**

* This edits the Windows registry.
* **fDenyTSConnections = 0** means **"allow remote desktop connections"**
* Registry path is where RDP settings are stored.

**Why it's useful:**

* Enables you to manage the server **remotely** (e.g., from your laptop), instead of working on a physical monitor.

****

**What it does:**

* Enables a **firewall rule** group called **"Remote Desktop".**
* Opens TCP port **3389** in the Windows Firewall so RDP connections can come in.

**Why it's useful:**

* Even if RDP is enabled, the firewall might block it. This ensures it’s allowed securely.