Implementation Guide: Basic Server Hardening

This guide provides simple, step-by-step instructions for securing your new server, matching the documentation sent to your manager.

Part 1: Create the Admin User

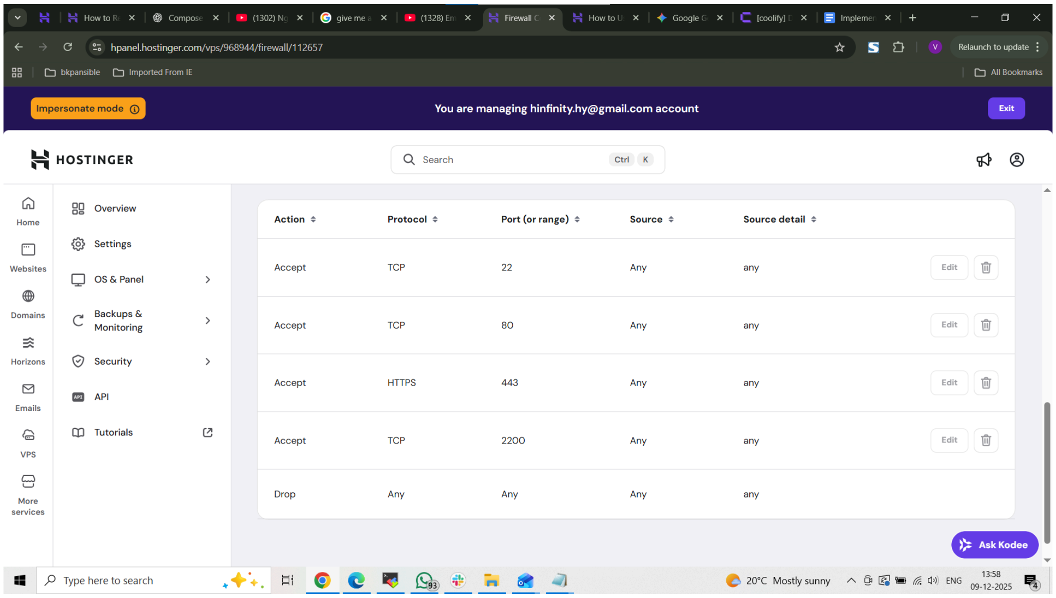
We stop using the powerful "Root" account and create a new user who must explicitly request permission (using sudo) to perform dangerous actions. We will use the username `hinfinityadmin` for this example.

1. **Create the user:**
   - `adduser hinfinityadmin`
   - *(Set a strong password when asked. Press Enter to skip the "Full Name" and other optional questions).*
2. **Give them power:**
   - `usermod -aG sudo hinfinityadmin`
3. **Test the power:**
   - Switch to the new user: `su - hinfinityadmin`
   - Run a test: `sudo ls /root`
   - *(If the command lists the files in the root directory, your user has the required power. Type `exit` to go back to the root account).*

Part 2: Setup the Firewalls

We must block all network access (ports) except for the few services we actively use.

1. **Hostinger Cloud Firewall (Do this in the Website Dashboard):**
   - Go to **VPS > Security > Firewall**.
   - **Add Rule:** Accept | TCP | Port 2200 | Source Any.
   - **Add Rule:** Accept | TCP | Port 80 | Source Any.
   - **Add Rule:** Accept | TCP | Port 443 | Source Any.
   - *(Make sure to DELETE the rule for Port 22 once you confirm 2200 works later).*

- 

hpanel.hostinger.com/vps/968944/firewall/112657

You are managing hinfinity.hy@gmail.com account

Action	Protocol	Port (or range)	Source	Source detail
Accept	TCP	22	Any	any
Accept	TCP	80	Any	any
Accept	HTTPS	443	Any	any
Accept	TCP	2200	Any	any
Drop	Any	Any	Any	any

2. **Internal Firewall (UFW):**
   Run these commands inside the terminal (as root):
   - `$ ufw default deny incoming`
   - `$ ufw default allow outgoing`
   - `$ ufw allow 2200/tcp` (For new SSH login)
   - `$ ufw allow 80/tcp` (For web traffic HTTP)
   - `$ ufw allow 443/tcp` (For web traffic HTTPS)
   - `$ ufw enable`
   - *(Type y and press Enter to confirm)*

Part 3: Secure the Login (SSH)

This step involves changing the login port and configuring secure login settings for your new user.

1. **Open the config file:**
   - `nano /etc/ssh/sshd_config`
2. **Change these lines:**
   - **Change Port (uncomment and modify):** `Port 2200`
   - **Allow Passwords (uncomment and modify):** `PasswordAuthentication yes`
   - **Disable Root (Pending Step, uncomment and modify):** `PermitRootLogin no`
3. **Save:** Press Ctrl+O, Enter, then Ctrl+X.

Part 4: The Fail2Ban

Fail2Ban monitors your server logs. If someone fails to log in multiple times, it temporarily bans their IP address.

1. **Install it:**
    - `apt update && apt install fail2ban -y`
2. **Configure it:**
    - `nano /etc/fail2ban/jail.local`
3. **Paste these settings:**

```
[sshd]
enabled = true
port = 2200
maxretry = 3
bantime = 10m
```

4. **Start it:**
    - `systemctl enable fail2ban`
    - `systemctl start fail2ban`

Part 5: Final Verification

Always perform this check **before** closing your current root terminal window.

1. **Restart SSH:**
    - `systemctl restart ssh`
    - *(If there are any errors, fix them before proceeding).*
2. **Open a NEW terminal window.**
3. **Try to connect:**
    - **User:** `hinfinityadmin`
    - **Port:** `2200`
    - **Password:** (The one you set in Part 1)
    - ssh `hinfinityadmin@<pubip> -p 2200`

If you successfully log in using the new port and the `hinfinityadmin` user, your server is secured! You can now close the old root window.