🛠 **Step-by-step:**

1. **Discover the IP:**
   Use VPN/provided info (or nmap).
2. **Discover the hostname** (if not given):
   - Check in the CTF question description
   - Or use:

bash

CopyEdit

gobuster vhost -u http://<IP> -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt

3. **Map IP to hostname locally:**
   Edit /etc/hosts:

bash

CopyEdit

sudo nano /etc/hosts

Add line like:

lua

CopyEdit

10.10.10.42 vuln-web.local

4. **Use the hostname in browser or curl:**

bash

CopyEdit

curl http://vuln-web.local/../../../../etc/passwd

🔎 **Tip to Detect Virtual Hostnames:**

- If accessing http://<ip> shows "default Apache page" or "Not Found"
- If curl to IP gives 404, but ports like 80/443 are open
- If nmap or nikto shows ServerName in response headers

That's usually a sign that it expects **Host header / virtual host**.

□ Add to Notes:

bash

CopyEdit

```
# Hostname not working in browser? Add to /etc/hosts
echo "10.10.10.42 vuln-web.local" | sudo tee -a /etc/hosts

# Access site using hostname
curl http://vuln-web.local

# Virtual host fuzzing (if hostname unknown)
gobuster vhost -u http://<IP> -w /usr/share/seclists/Discovery/DNS/namelist.txt
```