1.子域名

2.信息泄漏 如 phpinfo

3.邮箱找回 看邮箱头 ip

4.查看域名历史记录 (一个域名从无 cdn 到有 cdn 有个过程)
http://toolbar.netcraft.com

5.fuzz ip (通过前期的收集 用脚本绑定收集的 IP 去访问)

6.有能力可以扫下全网