入侵第1步就是踩点，相信有些经验的老鸟都知道，首先我们应该从网站入手，先谷歌下网站存在神马漏洞  site:xxxx.com inurl:asp?id=(php?id=)  
site:xxxx.com inurl:upload  
site:xxxx.com inurl:fck  
site:xxxx.com inurl:eweb  
site:xxxx.com inurl:login  
site:xxxx.com intext：管理的邮箱或者QQ，手机都可以  
用网站扫描器扫描下网站目录，看有神马可利用的  
查询下同服务器是否存在其他网站或者分站  
用这些收集完后整理一下，有漏洞的则以漏洞为突破口 ，没有则以旁站+社工为突破口，实在不行您老就C段ARP嗅探下，装了防火墙可以突破下  
不要小看踩点哦，很多不能拿下的网站都是这样被日下的哦  
其实踩点还有很多技术的，在这里就不一一解释咯，