**渗透中寻找突破口**

<http://static.hx99.net/static/drops/tips-2915.html>

### 1.网段信息

### 2.利用whatweb寻找web入口

### 3.利用nmap寻找可利用服务

### 4.利用搜索引擎寻找后台或重要系统

### 5.搞一个精简的路径字典