[toc]

网络侦察技术

问什么要信息收集

- 信息收集技术是一把双刃剑

  > 黑客在攻击准备之前需要收集信息，才能实施有效供给
  >
  > 管理员用信息收集技术来发现系统的弱点

- 信息收集是一个综合过程

  > 从一些社会信息入手
  >
  > 找到网络地址范围
  >
  > 找到关键的机器地址
  >
  > 找到开放端口和入口点
  >
  > 找到系统的制造商和版本

以太网卡的工作模式

- 网卡完成收发数据报的工作，一共有两种接受模式

  > 混杂模式：不管数据帧中的目的地址是否与自己的地址匹配，都接受下来
  >
  > 非混杂模式：

-

找老师技巧

- 老师一般不看第一封邮件，如果有意联系老师，一般多发几封邮件

  > 不要一封邮件多发，用心写

- 写清楚自己参与的项目中

  - **自己做了什么**
  - **自己获得了什么**

- 建议

  - 对老师的论文提出自己的见解

- 参与面试应该成为主导者，不要被动等待老师提问

  > **可以展开说自己擅长的部分**
  >
  > **不要怕说错**

- 形式上的东西要做好
    - 这是最不需要动脑子的

作业

- 有交换机的网络如何监听
-