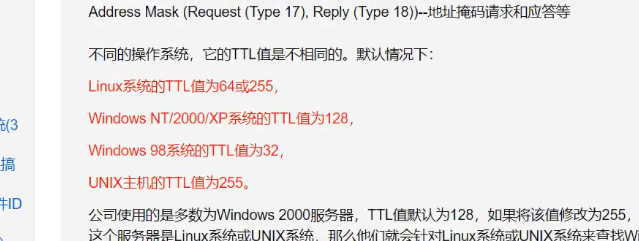
# 3.系统及数据库

1. 操作系统————系统层面漏洞、识别、漏洞类型
   1. windows
   2. 实例：msf攻击，开40端口即可
   3. linux
   4. 实例：判断操作系统类型
      1. 1.windows对大小写不敏感，linux会报错
      2. 2.nmap扫描（nmap -O ip）
      3. 3.ping 的TTL值不同，不准确



1. WEB
   1. 网站源码————CMS，框架或内部源码不同思路
      1. 内部或未知
      2. 开源CMS
      3. 框架和非框架
      4. 白盒代码审计，漏洞挖掘
      5. 部分漏洞采用人工辅助探针
   2. 搭建平台
      1. 配置导致安全问题
      2. 安全配置防护————中间件安全
         1. ip或用户验证
         2. 文件格式解析
         3. 目录或文件执行权限
         4. ……
   3. 数据库————数据库安全
      1. 脚本与数据库对应
         1. asp+access（只支持windows）
         2. php+mysql（3306端口）
         3. aasp+mssql（只支持windows）
         4. jsp+mssql，oracle（1521端口）
         5. python+mongdb（27017端口），mysql
         6. sqlserver（只支持windows）
         7. 实例：端口扫描区分数据库类型
      2. 弱口令
      3. 漏洞
   4. APP————系统漏洞，反编译提取url，抓包结合web
      1. android
      2. ios
   5. 第三方————常见的第三方软件或服务类安全问题
      1. openssh
      2. weblogic
      3. jboss
      4. redis
      5. serv-u
      6. phpmyadmin
      7. phpstudy
      8. ……